



سلامة أطفالنا
على شبكة الإنترنت

مادة تدريبيّة حول
سلامة الأطفال
على الإنترنت

سلامة أطفالنا
على شبكة الإنترنت

مادة تدريبيّة حول
سلامة الأطفال
على الإنترنت





تنسيق:

نهى أبي حبيب (المركز التّربوي للبحوث والإنماء)

تأليف الجزء الأوّل: الخلفيّة المعرفيّة للمعلّم.

غريس صوان (المركز التّربوي للبحوث والإنماء)

تأليف الجزء الثاني:

سيدة الأحمر (المركز التّربوي للبحوث والإنماء)

غريس صوان (المركز التّربوي للبحوث والإنماء)

كارمن شبيب (المركز التّربوي للبحوث والإنماء)

استشارة:

وسام قطيط (جمعيّة حماية)

ماريا برونيان (جمعيّة حماية)

أكرم كرامه

زينة الخوري (مؤسسة الرؤية العالميّة)

مقدّمة

في عصر التواصل العالمي المتعدد الوسائط الذي نعيش في خضمه ، أصبحت تكنولوجيا المعلومات والاتصالات تشغل حيّزًا كبيرًا من حياتنا وأنشطتنا اليومية، ولم تعد تقتصر على فئة عمرية معينة بل أصبح استخدامها متوافرًا للجميع، بحيث تحوّلت إلى عنصر حيوي من عناصر الإعلام وإلى حاجة جدية كمصدر للمعلومات، بالإضافة إلى أنها أصبحت أداة تعليمية مهمة للأطفال لدرجة أن عددا من المدارس أدخل استخدامها في المناهج الدراسية كوسيلة تربوية معاصرة إدراكاً منه لأهميّتها في مساعدة الأطفال على تنمية مهاراتهم الذهنية والعقلية ،وتعزيز قدرة الإبداع والابتكار والتحليل لديهم، بالإضافة إلى إكسابهم مهارات تساعدهم على التعامل مع البيئة والمجتمع والمحيط.

لذلك فإننا نشهد إقبالًا متزايدًا من الأطفال على استخدامها بسهولة ولكن للأسف الشديد من دون أي إشراف أو توجيه، فيصبح إبحار الطفل في هذا العالم الواسع كالسير وسط حقل محفوف بالمخاطر وهنا يكمن لبُّ المشكلة.
أمام هذا الواقع الخطير الذي أصبح سمة عالمية ، أنجز المركز التربوي للبحوث والإنماء مشروع «سلامة الأطفال على الإنترنت» بهدف توفير بيئة أكثر أمانًا، ورفع مستوى الوعي حول الاستخدام السليم والمسؤول للإنترنت لدى الأطفال والأهل ومقدمي الرعاية في آن معًا، وذلك انسجامًا مع السياسة التربوية التي بُنيت على أساسها خطة النهوض التربوي في لبنان، والتي تعتبر أن التربية وسلامة الطفل الجسدية والعقلية والنفسية هي مسؤولية مشتركة بين الأسرة والمجتمع والدولة.

إن الأثمان الباهظة التي تترتب على مجتمعنا حاضرًا ومستقبلًا نتيجة لهذه الأخطار الكبيرة التي يواجهها أطفالنا في خلال عملهم المباشر على الشبكة بلا توعية مسبقة أو إرشاد من الأهل أو ذوي الرعاية، هي التي شكلت خلفية هذا المشروع وفرضت نفسها على المركز التربوي للبحوث والإنماء كمؤسسة تربوية وطنية معنيّة بالإنماء التربوي الذي محوره الإنسان، كما تفرض نفسها أيضًا على المؤسسات الأخرى أكانت اجتماعية أم وطنية أم دولية لتحقيق شراكة هادفة في مجال توعية الرأي العام، وتزويد جميع مقدِّمي الرعاية للأطفال بالمعارف والمهارات والمواقف الضرورية وتأهيلهم لدعم هذا المشروع وتطبيقه في شكل فعّال، وتوعية الأطفال وإرشادهم بهدف تمكينهم من اكتساب القدرة على حماية أنفسهم، وتثقيف الأهل عن طريق العاملين في هذا المجال لبناء القدرة على التواصل والحوار والتفاهم بين الأطفال وذويهم بغية تأمين بيئة أكثر سلامة للأطفال على الشبكة.

وإننا إذ نضع ما أنجزناه بين أيدي الإدارات المدرسيّة والأساتذة والأهل والأطفال ليكون الموجّه المناسب لحسن التعاطي مع العالم الرقمي، فإننا على ثقة بأن تعميم هذا المشروع والعمل بهدْيِه سيكون بين أيدي أمينة حفاظًا على مستقبل أطفالنا وسلامتهم.

رئيسة المركز التربوي للبحوث والإنماء

الدكتورة ليلى فياض

الفهرس

الجزء الأوّل: الخلفيّة المعرفيّة للمعلّم

الجزء الثاني: الأنشطة

الجزء الأوّل: الخلفيّة المعرفيّة

أهداف المادّة التّدريبيّة

الهدف العام:

خلق بيئة أكثر أمانًا لضمان سلامة الأطفال عند استخدامهم للإنترنت في لبنان.

الأهداف الخاصّة:

الهدف ١: رفع مستوى الوعي العام حول فوائد استخدام الإنترنت، وتأثير مخاطر استعماله السّيّء في نموّ الأطفال وسلامتهم.

الهدف ٢: رفع مستوى الوعي عند الأطفال، وتمكينهم من الإبحار السّليم والآمن على شبكة الإنترنت.

الهدف ٣: تطوير مهارات وقدرات مقدّمي الرّعاية للأطفال (من مربّين، مرشدين اجتماعيّين، ...) لتمكينهم من مساعدة الأطفال على الاستخدام الآمن والمسؤول للإنترنت.

الهدف ٤: توعية الأهل وتثقيفهم لخلق بيئة أكثر أمانًا لضمان سلامة الأطفال على الإنترنت، وتشجيعهم على فتح باب الحوار المستمر مع أولادهم حول استخدامهم السّليم للإنترنت.

الفوائد الّتي يجنيها الأطفال من الإنترنت

يستخدم الإنترنت أكثر من ملياري شخص حول العالم لغايات متنوعة منها اكتساب المهارات، التّجارة، التّسوّق، تبادل المعلومات، التّسلية والتّرفيه، تتبّع الأخبار والتّواصل ...وإنّ إقبال الأطفال على استخدامه يتميّز بمرونة وحماس أكثر منه لدى الكبار. فالطّفل لديه فضول بطبيعته وهذه الأداة ترضي فضوله لما تُوفّره له من ألعاب ومعلومات.

تُعتبر شبكة الإنترنت مصدرًا غنيًّا للحصول على المعلومات والمعارف، وهي عبارة عن أداة تعليميّة محفّزة ومسلّية للأطفال، حيث يمكن مشاهدة المعارف المفيدة تعلّمها وحلّ المسائل من خلال الألعاب والبرامج التّثقيفيّة والشّبكات الاجتماعيّة. ناهيك عن كونها مصدرًا للتّواصل بين الأشخاص ما يوفّر فرصًا للتّعلم من طريق تبادل المعلومات والمعارف والأفكار وإمكانيّة عرض التّساؤلات على عدد كبير من الخبراء والباحثين في مختلف المواضيع الّتي تتّصل بالمقرّرات الدّراسيّة.

وتخلق الشّبكة جوًّا من التّفاعل والمشاركة بفضل ما توفّره من وسائل للتّواصل الاجتماعي مع الأقران والأصدقاء والعائلة داخل النّطاق الجغرافي الّذي يعيش فيه الطّفل أو خارجه وذلك عبر البريد الإلكترونيّ والرّسائل الفوريّة والشّبكات الاجتماعيّة وغيرها... كما تنمّي مهارات البحث، التّحليل، الاستنتاج، التّفكير النّقدي، الإنتاج الابداعي، والقدرة على التّفكير السّليم والتعلّم الذاتي من خلال أساليب البرمجة الّتي تتّسم

بالمنطقيّة، والتّخطيط السّليم من جهة، وما تقدّمه من مواضيع ومعلومات وبين ما يكتشفه الطّفل بنفسه من جهة أخرى، إضافة إلى تنمية مهارات استخدام الحاسوب في المشكلات والمواقف التّعلّميّة. كما تنمّي هواية المطالعة لدى الطّفل بفضل احتوائها على عدد لا متناهٍ من المواقع المهمّة الّتي تمتاز بجودة نوعيّة المادّة الّتي تقدّمها، وبالتّصميم المميّز، والمثير للاهتمام والفضول، ما يجعل من تصفّحها مصدرًا للتّمتّع والتّسلية واكتساب المعرفة في آن معًا.

وبالإضافة إلى ما تمّ ذكره أعلاه، فإنّ الشّبكة تؤمّن أيضًا بيئة تعلّم محفّزة ومثيرة للطّلاب، مستمدّة من واقعهم الاجتماعي. إذ تُشركهم في التّعبير عن آرائهم من طريق الشّبكات الاجتماعيّة، والمدوّنات، ومنتديات المناقشة الّتي توفّر لهم إمكانيّة تدوين مواضيع اهتماماتهم، ومناقشة القضايا ووجهات النّظر، والمشاركة في طلب المشورة أو تقديمها لمن يحتاجها.

سلامة الأطفال على الإنترنت:

في غياب ضوابط استخدام شبكة الإنترنت تكثر فرص تعرّض المستخدم للمضايقات، وفي بعض الحالات تصل إلى حدّ حصول ضرر كبير له.

لذا يقول أحد الخبراء: «إبحار الطّفل عبر الشّبكة يشبه سيره في حقل للألغام، والتّنقل عبر المواقع الإلكترونيّة العاديّة قد يؤدّي إلى متاهات صادمة ومضرة بكلّ المقاييس» وعلينا أن نعي المخاطر الّتي تحدق بالأطفال ونحرص على مناقشتها معهم.

وهنا لابدّ لنا أن نفهم إيجابيّات استخدام الإنترنت وسلبيّاته، ونناقش ذلك مع أطفالنا، ونتبع بعض المبادئ التّوجيهيّة، لنجعلهم يستمتعون بتجربة أكثر أمانًا وسلامة على الإنترنت.
ويمكن تقسيم سلامة الأطفال على الشّبكة إلى أربعة أنواع:

١- السّلامة الجسديّة:

السّلامة الجسديّة هي كلّ تعرّض لأذى جسدي أو عنف، مثل:

التّحرّش بالأطفال:

يقوم الأطفال، ولا سيّما من هم في سن ما قبل المراهقة أو المراهقة، عند تصفّح الإنترنت، بتكوين صداقات والتّعرّف بأشخاص جدد من خلال الشّبكات الاجتماعيّة المثيرة بالنّسبة إليهم وذلك بسبب سمة التّخفّي، والسّرّيّة الّتي تتميّز بها، وميلهم إلى عنصر المغامرة الّذي يُعتبر جزءًا من عمليّة نموّهم. ويؤدّي تواصلهم المباشر مع هؤلاء الغرباء، الّذين قد يكونون منحرفين، إلى الكشف عن معلومات قد تُعرّضهم أو تعرّض أسرتهم إلى خطر شخصيّ.

وأحيانًا يتمّ إغراء الأطفال بالالتقاء خارج الفضاء الافتراضي. ويمكن للقاءات من هذا النّوع أن تهدّد سلامتهم. فالمتحرّشون بالأطفال يستخدمون بشكل خاص غرف الدّردشة، والمنتديات، وبرامج المراسلة الفوريّة لكسب ثقتهم، وانتزاع معلومات شخصيّة منهم بطرق ماكرة، وترتيب لقاءات وجهًا لوجه بهدف الاستغلال الجنسي. والجدير بالذّكر أنّ المتحرّشين بالأطفال لا يتبعون الطّرق نفسها للإيقاع بضحاياهم، ولكن غالبًا ما يستخدمون الأساليب الآتية:

- **الاستدراج:** وهي عمليّة التّلاعب الّتي يقوم بها المتحرشون لترتيب لقاء حقيقي مع الأطفال بهدف الاعتداء عليهم. فهم يرون عمليّة تعقّب الأطفال والإيقاع بهم كلعبة صيد، ويمضون الكثير من الوقت، وعلى مدى أشهر وسنوات عدّة وبطرق ماكرة، لكسر الحواجز بينهم وبين ضحاياهم، وكسب ثقتهم من خلال مدّهم بما يحتاجون إليه من عطف، واهتمام، وهدايا، لجعلهم يشعرون بأنهم محبوبون ومرتاحون.
ويكون المتحرّشون على علم بأحدث أنواع الموسيقى، والأفلام، والألعاب، والأنشطة الّتي تثير اهتمام الضّحايا، وبمجرد كسب ثقتهم يدرجون المحتوى الجنسي شيئا فشيئا في محادثاتهم معهم.

- **الدّردشة على انفراد:** إذا كان المتحرّش يتواصل مع الضّحيّة في غرفة دردشة عامّة فإنّه يطلب إليها التّحدّث عبر غرفة دردشة خاصّة private chat room أو من طريق الهاتف أو الرّسائل النّصّيّة sms.

- **الإطراء :** يستخدم المتحرّشون الاهتمام الزّائد، والتّملق، والمديح المبالغ فيه للإيقاع بضحاياهم، وأحيانًا يدّعون وقوعهم في الحبّ ويغدقون عليهم وعودًا بالشهرة، وتقديم فرص عمل في عرض الأزياء أو التّمثيل أو الغناء مثلا، وفي حال تجاوب الضّحايا يستدرجونهم شيئًا فشيئًا لتحقيق غاياتهم كالطّلب إليهم أخذ صور إغرائيّة وإباحيّة بحجّة عرضها على وكالة عرض أزياء على سبيل المثال لا الحصر.

- **التّرهيب:** بمجرّد أن يتعرّف المتحرّش إلى الضّحية، ويصبح لديه معلومات ومحتويات قابلة للابتزاز والتّهديد، فإنّه يبدأ بالتّهديد والتّخويف بنشر صور معيّنة، أو بإخبار الأهل والأقرباء بأمر ما.

- **التّحايل للحصول على معلومات شخصيّة:** يحاول المتحرّشون انتزاع معلومات شخصيّة عن الأطفال تساعدهم على الإيقاع بهم. وهذه المعلومات لا تقتصر فقط على الاسم، والعنوان، ورقم الهاتف، بل تتعدّاها إلى معرفة الأماكن الّتي يرتادها هؤلاء الأطفال كالمدرسة، دور السّينما، النّوادي، الملاعب أو الحدائق العامّة. فبذلك يكونون على اتصال مباشر بهم من دون أن يتعرّف إليهم أحد، وبعيدًا عن الأماكن الّتي تعرّضهم لخطر التعرّف إليهم كالمنزل أو الشّارع الّذي يسكنونه. وتعتبر جملتان مثل: «أنا ذاهب إلى النّادي لألعب كرة السّلة»، و«بعد ممارسة الرّيّاضة أحبّ أن أتمشّى وأرتاح في الحديقة المجاورة»، كافيتين لتحديد مكان الطّفل من دون ذكر اسم النّادي أو الشّارع. وأغلب الأطفال الضّحايا تمّ الإيقاع بهم خلال فترات الاستراحة أو خلال عودتهم إلى المنزل.

- **التّعاطف:** يدّعي المتحرّش بتطابق حالته مع الحالة الّتي يمرّ بها الطّفل، ويقوم بتقليد لغته، على سبيل المثال إذا كان الطّفل وحيدًا، أو منبوذًا من رفاقه، أو لديه مشاكل مع أهله يخبره بأنّه يتفهّم الأمر، لأنّه يمرّ بالحالة

نفسها، ويودّ أن يكون صديقه، والملاحظ أنّ أغلبيّة المراهقين يشعرون بأنّ لا أحد يفهمهم، ويبحثون عن التّعاطف والدّعم على الإنترنت، ويستغلّ المتحرّش هذه الحالة لكسر الحواجز بينه وبين الضّحيّة، وخلق صداقة حميمة وهميّة، وملء الفراغ.

علامات تنبّه بأنّ الطّفل يتعرّض للإستدراج من قبل متحرّش:

- الاضطراب والسرّيّة الّتي يُظهرها الطّفل عندما تفاجئه وهو يستخدم الإنترنت مثل: غلق الشّاشة إذا ما اقتربت منه فجأة، أو أيّ سلوك آخر يدلّ على أنّه لا يريدك أن تعرف شيئًا عن أنشطته على الشّبكة.
- تمضية الكثير من الوقت في غرف الدّردشة.
- القيام باتصالات هاتفيّة، وتلقّي اتصالات أو رسائل نصّيّة من أرقام غريبة لا تعرفها.
- تلقّي بريد أو طرد من خارج البلاد أو من أشخاص غرباء.

على الطّفل أن يفهم أنّها ليست مسألة مراقبة، ولا مسألة ثقة، وإنّما هي مسألة اهتمام بسلامته فحسب، شأنها شأن منعه من قيادة الدّراجة في أماكن خطرة.

٢- السّلامة النّفسيّة:

السّلامة النّفسيّة هي كلّ تعرّض لمضايقات وتهديدات أو محتوى مزعج.

• التّعرّض لمحتوى غير لائق:

محتوى الإنترنت غير خاضع للرّقابة تمامًا، لذا يمكن أن يتعرّض الأطفال إلى محتوى غير لائق بسبب إمكانية الوصول بسهولة إلى المواقع الإباحيّة الّتي تروّج للعلاقات الجنسيّة غير المسؤولة، ما يؤدّي إلى الإصابة بالأمراض الجنسيّة التّناقليّة أي Sexually Transmitted Dieseases STD، كما ويخلق مفاهيم مغلوطة عن الجنس في ذهنهم. هذا فضلاً عن نشر محتويات عنصريّة، عنيفة، مشجّعة على الإنتحار، وتعاطي المخدّرات، والكحول، ومروّجة لعلاجات ومستحضرات مضرّة بالصّحّة، وغير معترف بها طبّيًّا. بالإضافة إلى مواقع البيع غير المشروع للأسلحة، والبضائع المسروقة والمخدّرات، أو معلومات حول إعداد المتفجّرات وذلك عبر المواقع الإلكترونية، البريد الإلكتروني، غرف الدّردشة، الرّسائل الفوريّة والمنتديات. ناهيك عن الألعاب العنيفة والّتي تحوي مشاهد دمويّة أو غيرهامن المشاهد الّتي لا تلائم نموّ الطّفل، وتؤثّر سلبًا ليس فقط في نمّوه الذّهني بل أيضًا في سلوكيّاته وتصرّفاته مع الآخرين.

هناك الكثير من الأساليب التي تهيّئ لحماية الأطفال وتجنّبهم التّعرّض للمواقع غير المرغوب بها كالمواقع الإباحيّة وغيرها من المواقع غير المناسبة، ومن هذه الوسائل نذكر البرامج الّتي تتيح رقابة أبويّة على الإنترنت والّتي تُستخدم لمنع برامج ومواقع معيّنة وصدّها.

لذا تقع على عاتق الأهل مسؤوليّة مراقبة تحرّكات أطفالهم على الشّبكة وتعقّبها، والتّعرّف إلى طبيعة المواقع الّتي يزورونها، ومراكز اهتمامهم وأنشطتهم على الشّبكة من طريق استخدام برامج الفلترة والمراقبة

الأبويّة Filtering and Parental Control Software الّتي تسمح بمراقبة البرامج غير المرغوبة وتصفيتها، ولكن إلى حد ما، ولا تستهينوا بقدرة الأطفال على تعطيل هذه البرامج.

• التّهديد والمضايقة والابتزاز:

قد يتعرّض الأطفال إلى محتويات مزعجة، مهينة، محرجة أو عدوانيّة تصلهم عبر رسائل البريد الإلكتروني أو في غرف الدّردشة، وتتحوّل هذه المواقع إلى أماكن خطرة إذ لا يمكن أن نعرف هويّة جميع المشاركين في المحادثة، لذا فمن السّهل ابتزاز شخص ما أو مضايقته من طريق تشويه صورة ما له أو تهديده بنشر معلومات شخصيّة أو صور محرجة، وعندما يتجاوز الأمر حدّه ينبغي إبلاغ الشّرطة.

ليس من الضّروري أن يكون الطّفل هو الضّحيّة دائمًا، بل يمكن أن يكون هو من يقوم بإرسال التّهديدات، لذا عليه أن يعرف بأنّ هذا السّلوك غير مقبول، وله عواقب منزليّة وقانونيّة وفي حال حاول إخفاء هويّته الحقيقيّة فينبغي أن يعي أنّه توجد طرق عدّة لتعقّب الفاعل والكشف عن قناعه.

• التّنمّر السّيبراني CYBERBULLYING:

لم تقتصر ممارسة التّنمّر على البيئة الواقعيّة، بل امتدّت إلى فضاء الإنترنت والتّجمعات الافتراضيّة. والبلطجة السّيبرانيّة أو التّنمّر السّيبراني عندما يقوم طفل أو مراهق بالإساءة إلى طفل أو مراهق آخر من طريق إرسال: تهديدات، أو رسائل وصور عدائيّة، أو الإفصاح عن معلومات شخصيّة وحسّاسة، أو تَعمُّد استبعاد الضّحيّة من مجموعة معيّنة على الشّبكة، أو شنّ حملات ضدّه، أو المضايقة، أو الإحراج، أو السّخرية، أو الإهانة وتشويه السّمعة، أو إطلاق إشاعات، أو تشويه الصّور ونشرها عبر المواقع الاجتماعيّة مثل Facebook، غرف الدّردشة، منتديات النّقاش Discussion Forums، البريد الإلكتروني، الرّسائل الفوريّة، الهواتف المحمولة، صفحات الويب والمدوّنات Blogs... وبعضهم قد يسيء أو يعتدي على الطّفل حتّى يشعر بالإحباط ويفقد احترامه لذاته وثقته بنفسه. ويمكن لأيّ طفل أن يفعل ذلك مع الآخرين كونه يشعر بأنّه محمي وراء الشّاشة.

الضّرر الّذي يتسبّب به التّنمّر السّيبيراني كبير، ويعود ذلك إلى عدّة أسباب نذكر منها:

- سرعة انتشار المحتوى عبر الشّبكة.
- ارتفاع نسبة المشاهدين: لا سيّما إذا كانت الصّفحة تضم عددًا من الأصدقاء وزملاء المدرسة والمعارف والأقارب ما يزيد من حالة الإحراج والإذلال الّتي تشعر بها الضّحيّة.
- توافر إمكانيّة الاحتفاظ بالمحتوى: كلّ من وصل إلى المحتوى يستطيع أن يحتفظ به ما يضاعف الضّرر النّفسي والمعنوي الّذي يتعرّض له الطّفل في حال عاود معاينة المحتوى بنفسه أو تمّ إعادة عرضه من قبل شخص آخر.
- الشّبكات الإجتماعيّة: تسمح هذه الشّبكات، من خلال الخدمات الّتي تقدّمها، بشنّ حملات ضدّ شخص معين ويستخدم البلطجيّون هذه الخدمات لإهانة ضحاياهم والإساءة إليهم مثلاً: حملة انتخاب أقبح و/أو أغبى و/أو أسوأ طفل في الصّفّ، ودعوة المشاهدين إلى التّصويت أو التّأييد أو التّعليق على الموضوع .

وقد أظهرت الدّراسات أنّ التّنمّر يترك آثارًا نفسيّة سلبيّة ومؤذية على الضّحيّة منها: الحزن، الخجل، القلق، الخوف، الاكتئاب، التّراجع في المستوى الأكاديمي، العزلة الاجتماعيّة، الشّعور بالعار، فقدان الثّقة بالنّفس، الإحباط، الغضب، والرّغبة الشّديدة في الانتقام، وقد تؤدّي في الحالات القصوى إلى الانتحار أو ارتكاب جريمة.

بعض النّصائح للأطفال في حال التّعرّض للتّنمّر السّيبيراني:

١. الاحتفاظ بالأدلّة كالرّسائل، الصّور، الفيديو، التّعليقات، البريد الإلكتروني... فقد تدعو الحاجة إليها لاحقًا لإثبات الفعل.
٢. إبلاغ شخص راشد من الأهل أو الأقارب أو المربّين.
٣. صدّ المتنمّر block وعدم الرّدّ على أيّ من إساءاته، وتجنّب قراءتها.
٤. الاستفادة من خدمة الإبلاغ عن الإساءة الّتي توفّرها معظم الشّبكات الاجتماعيّة، وخدمات البريد الإلكتروني وغيرها.
٥. التعرّف إلى هويّة المتنمّر ومواجهته: هناك طرق عدّة لتعقّب المتنمّر، والتّعرّف إليه في حال إخفاء هويّته، سواء من طريق مزوّد الخدمات service provider في المواقع الّتي تعرّض فيها الضّحيّة للإساءة أو من خلال الاستعانة بتقني لتعقّب عنوان الـIP.

اقتراحات للمربيّن حول كيفية التّعامل مع التّنمّر السّيبيراني في المدارس:

- حدّثوا الطّلاب عن التّنمر السّيبيراني.
- استحدثوا قوانين وتدابير وعقوبات في النّظام المدرسي لمكافحة التّنمر بأنواعه ومنها السّيبيراني.
- باشروا بالتّحقيق الفوري في تقارير التّنمر السّيبيراني.
- أعلموا أهالي الضّحايا وأهالي المتنمّرين، وحاولوا حلّ المشكلة ضمن حرم المدرسة في حال كان المتنمّر والضّحيّة ينتميان إلى المدرسة نفسها.
- أبلغوا الشّرطة في حال الشّكّ بوجود خطر على الضّحيّة.
- راقبوا عن كثب سلوك الطّلّاب تحسّبًا لاحتمال حدوث تنمّر.
- استخدموا بعض الدّعم من المرشدين في علم النّفس المتوفّرين في المدرسة.

اقتراحات للأهل حول التّعامل مع التّنمّر السّيبيراني:

- لا تتسامحوا مع التّنمّر في البيت، واشرحوا لأطفالكم بأنّ أخلاقيّات التّعامل مع النّاس في الحياة الحقيقيّة تنطبق أيضًا على الإنترنت والهواتف المحمولة.
- تحدّثوا إلى أطفالكم عن احترام الآخرين وأوضحوا لهم بأنّ التّنمّر السّيبيراني هو سلوك سيّء وغير مقبول، وأنّ هناك عواقب وخيمة لمثل هذا السّلوك، سواء أكان في البيت أم في الخارج.
- شجّعوا أطفالكم على أن يكونوا صريحين معكم في حال وقوعهم هم أو أيّ شخص من محيطهم ضحيّة التّنمّر السّيبيراني أو أيّ سلوك مزعج على الشّبكة.
- حذّروا أطفالكم من تشارك كلمة السرّ أو أيّة معلومات شخصيّة مع أيّ من رفاقهم، أو إعارة حاسوبهم

الشّخصي أو هواتفهم النّقّالة لأيّ كان منعًا من استغلال المحتوى بهدف الإساءة إليهم.

- شجّعوا أطفالكم على عدم الاستجابة لهذا السّلوك أو الرّدّ عليه.
- لا تحذفوا الرّسائل أو الصّور بل احتفظوا بها كأدلّة احتياطيّة.
- حاولوا التّعرّف إلى الشّخص الّذي قام بهذا الفعل: في حال كان من زملاء المدرسة أو من المعارف فمن الأفضل إعلام أهل المتنمّر وحل المشكلة مع الأهل، واتصلوا بالشّرطة في حال الضّرورة أو في حال اكتشاف نوايا سيئة.
- ضعوا الحاسوب في مكان عامّ في البيت وحدّدوا مدّة استخدام الشّبكة والتّوقيت، فالتّنمّر السّيبراني cyber bullying غالبا ما يحدث في وقت متأخّر من اللّيل بعيدًا عن الأنظار.

• الإدمان على الإنترنت:

الإدمان على الإنترنت هو الاستخدام المَرَضِيُّ للشّبكة والّذي يؤدّي إلى اضطرابات في السّلوك، وهي ظاهرة منتشرة لدى جميع المجتمعات في العالم بسبب توافر الحواسيب والإنترنت في كلّ بيت تقريبًا.

يتسبّب الإدمان على الشّبكة بمشاكل صحّيّة ونفسيّة منها اضطرابات في النّوم، تراجع في المستوى الأكاديمي، والعزلة الاجتماعيّة، ومن أسبابه: الملل، الفراغ، الوحدة، المغريات الكثيرة والمتنوّعة الّتي يوفّرها الإنترنت، ويتناول بشكل عام مكوّنات معيّنة وهي:

- الإدمان على مشاهدة المواد الإباحيّة.
- الإدمان على الألعاب والقمار.
- الإدمان على التّعارف وبناء العلاقات من خلال الشّبكات الإجتماعيّة، غرف الدّردشة، مواقع التّعارف أو برامج الرّسائل الفوريّة.
- الإدمان على التّحميل الزّائد للمعلومات من الشّبكة.

بعض النّصائح من أجل تفادي إدمان الأطفال على الإنترنت:

١- الإبقاء على التّوازن بين مختلف أنشطة الطّفل من خلال التّشجيع على اهتمامات وأنشطة اجتماعيّة أخرى، مثل القراءة وممارسة الرّيّاضة، وغير ذلك حتّى لا يمضي كلّ وقته بتصفّح الإنترنت في غرف الدّردشة وأمام الكمبيوتر، وإن اختل هذا التّوازن بشكل كبير لصالح الأنشطة الرّقميّة عندها يجب التّنبّه إلى وجود خطر الابتعاد عن المجتمع، وتقلّص فرص الإبداع.

٢- وضع قواعد واضحة لتحديد وقت استخدام الشّبكة والمدة.

• العلاقات العاطفيّة على الإنترنت:

تنتشر ظاهرة العلاقات الرّومانسيّة بكثرة على شبكة الإنترنت وهي ليست حكرًا على عمر معيّن بل تطول مختلف الأعمار، وغالبًا ما تنشأ علاقات مع أناس ليسوا من الفئة العمريّة نفسها للطّفل. وفي كثير من الحالات، يؤدّي هذا الفعل إلى عواقب وخيمة منها الابتزاز، والتّعرّض لمحتوى جنسي شاذ أو غير ملائم لسنّه، وقد تصل إلى حدّ التّحرّش والاعتداء الجنسي.

٣- سلامة السّمعة

سلامة السّمعة هي كلّ تشهير على الصّعُد الاجتماعيّة، والمهنيّة، والقانونيّة، والأكاديميّة. مثل:

• SEXTING:

ال Sexting هو تبادل المراهقين في ما بينهم رسائل تتضمّن عبارات جنسيّة فاضحة، أو تمرير صور عارية، أو نصف عارية (ملابس داخلية) أو ملفّات فيديو قصيرة لمشاهد إباحيّة لهم أو لزملائهم من طريق الهاتف المحمول أو الإنترنت (البريد الإلكتروني، أو الفايس بوك...).
يتسبب هذا الفعل بعواقب قانونيّة ونفسيّة وخيمة:

• **العواقب القانونيّة:** إن أخذ أو إرسال أو تمرير أو الاحتفاظ بصور عارية أو ملفات فيديو على الهاتف المحمول أو الإنترنت يعرّض الفاعل للملاحقة القانونيّة بتهمة إنتاج أو توزيع أو حيازة مواد إباحيّة للطّفل Child Pornography.

• **العواقب النّفسيّة:** نذكر منها تشويه السّمعة، التّشهير، الشّعور بالإحراج، العزلة الاجتماعيّة... لا سيّما في حال تمّ نشر هذه الملفّات على الشّبكة أو تمّ إرسالها إلى الأصدقاء، المعارف أو الأقارب ويعود السّبب في أكثر الأحيان إلى الرّغبة في الانتقام بعد فسخ علاقة غراميّة أو خلاف بين أصدقاء.

نصائح للأهل:

١. تحدّثوا إلى أولادكم عن الsexting وعواقبه، أوضحوا لهم أنّ هذا الفعل غير قانوني، ويجرّمهم بتهمة حيازة أو توزيع أو إنتاج مواد إباحيّة للطفل في حال أخذوا صورًا عارية لهم أو لأيّ شخص آخر أو قاموا بإرسال هذه الصّور والملفّات أو تمريرها أو الاحتفاظ بها.
٢. فسّروا لهم عن إمكانيّة استغلالها لابتزازهم والتّشهير بهم، وتشويه سمعتهم، وإذلالهم والانتقام منهم، وأنّ نهاية الصّداقات والعلاقات ليست كلّها سعيدة، حتّى ولو بدت مثاليّة في البداية. وبناء عليه يتوجّب عليهم ألّا يستجيبوا وألّا يشاركوا بهذا الفعل تحت أيّ ضغط كان، سواء أكان من الأصدقاء أو من أيّ شخص آخر .
٣. في حال قام أحد أولادك بأخذ صور عارية له أو إرسالها، حاولوا أن تهدأوا قبل كلّ شيء وتسيطروا على أعصابكم، ومن ثمّ حاولوا قدر المستطاع أن تستعلموا عن القصّة بكاملها، ثمّ اطلبوا إليه أن يتوقّف عن إرسالها لأحد وعلى الفور. وفي حال أرسلها إلى صديق أو حبيب تكلّموا إلى ذويه، وحاولوا معا إيجاد حل للمشكلة قبل أن تتفاقم الأمور، أما في حال اكتشاف نوايا سيّئة وخبيثة فأبلغوا الشّرطة فورًا.

نصائح للأطفال لا سيّما المراهقين:

١. ارفضوا رفضًا باتًّا، وتحت أيّ ضغط من صديق أو حبيب أن تقوموا بأخذ صور عارية لكم أو لغيركم أو إرسالها عبر الهاتف أو الإنترنت (webcam، بريد إلكتروني، رسائل فوريّة...).

٢. إن وصلتكم أيّة صورة أو ملف فيديو إباحي احذفوه على الفور، ولا ترسلوه أو تمرّروه لأحد. وفي حال وصل إليكم من خلال صديق أو شخص تعرفونه، تحدّثوا إليه وأعلموه أنّ ما يفعله غير قانوني وسيعرّضه لمشاكل مع الشّرطة، وبهذا تكونون قد أسديتم له خدمة. وإن لم يستجب لنصائحكم أخبروا شخصًا راشدًا ليتحدث إلى ذويه.
٣. في حال قمتم بأخذ صورة عارية لكم في السّابق وإرسالها لأحد ما لا تخافوا بل أخبروا شخصًا راشدًا ليحلّ المشكلة قبل أن تزداد الأمور سوءًا وتخرج عن السّيطرة.
٤. فكّروا جيّدًا في عواقب هذا الفعل مثل استغلال هذه الموادّ للتّهديد أو الابتزاز أو الانتقام أو تشويه السّمعة. وتذكّروا دائمًا أنّ نهاية الصّداقات والعلاقات ليست كلّها سعيدة، فقد يقوم صديق أو حبيب سابق باستغلال هذه الصّور رغبة منه في الانتقام أو الابتزاز.

• انتهاك القوانين:

هناك الكثير من الموادّ الموجودة على الشّبكة تملك حقوق الطّبع والنّشر، منها الموسيقى، والرّسومات، والفيديو، والنّصوص، لذا فإنّ عمليّة إعادة نشر أو طباعة هذه المواد، أو تقديم نسخ للأصدقاء، أو استخدام هذه النّصوص في المشاريع المدرسيّة من دون إذن المالك، ومن دون الاستشهاد بالمصادر الصّحيحة، تُعَدّ انتهاكًا لحقوق الملكيّة الفكريّة والأدبيّة، وبما أنّ هذا الفعل هو غير قانوني فإنّه يعرّض الفاعل للملاحقة القانونيّة.

• محاذير سياسيّة:

تقوم بعض الجماعات المتطرّفة أو المنظّمات باستغلال حماس المراهقين كوسيلة لتحقيق أهداف قوميّة، وسياسيّة معيّنة من طريق المحتويات والأفكار التي تبثّها على مواقعها فاقتضى التّوضيح. فليس بالضّرورة أن يكون كلّ ما ينشر على الشّبكة صحيحًا، لذا يستوجب عليهم ألّا ينجرّوا وألّا يتحزّبوا لأفكار وتيّارات سياسيّة معيّنة، وينبغي أن يتدرّبوا على التّفكير السّليم والمنطقي وتوقّع الغايات من كلّ محتوى.

٤- سلامة الهويّة والمعلومات الشّخصيّة والممتلكات

• استغلال المعلومات الشّخصيّة:

المتحرّشون بالأطفال، القراصنة، والمتربّصون، وبعض المواقع، والمنظّمات التّجاريّة كل هذه الجهات تسعى لانتزاع معلومات شخصيّة منهم. مثل الاسم، العمر، عنوان المنزل أو المدرسة، عنوان البريد الإلكتروني، رقم الهاتف، رقم بطاقة الائتمان والحساب المصرفي، ومعلومات متعلّقة بالبنية الجسديّة، وصور... مستخدمة أساليب متنوعة وماكرة منها مثلاً: ضرورة التّسجيل في مسابقة ما، أو تعبئة نماذج من أجل الحصول على جوائز أو الحصول على حق تحميل برامج أو ألعاب، أو إرسال السّيرة الذّاتية للحصول على فرص عمل... وفي حال ضرورة التّسجيل علينا مساعدة الأطفال على اختيار اسم مستخدم، ومعلومات وهميّة، حيث لا يكشفان عن أيّة معلومات شخصيّة تخصّهم.

في أغلب الأحيان يُستخدم هذا النّوع من المعلومات لأغراض تجاريّة، وفي الحالات الأكثر خطورة لإغراء الأطفال واستغلالهم وارتكاب جرائم جنسيّة، وماليّة، وسرقة الهويّة، والحسابات الشّخصيّة على الإنترنت مثل حساب البريد الإلكتروني والشّبكات الإجتماعيّة.

لذا علينا أن نساعد الطّفل على:

- الاستفادة من أدوات الخصوصيّة privacy settings للتّحكّم بخصوصيّة معلوماته وتحديد جمهوره...
- تجنّب الإفصاح عن أيّة معلومات شخصيّة تخصّه أو تخصّ أفراد عائلته أو زملاءه أو أي شخص آخر. وتحذيره من مخاطر نشر صور ومقاطع فيديو له على الإنترنت، لا سيّما في غرف الدّردشة، ومواقع الشّبكات الإجتماعية، والمنتديات forums، وأخبار المجموعات newsgroup، والمدوّنات blogs، إذ يمكن للمتحرّشين أو المتسلّلين أن يقوموا بجمع معلومات شخصيّة عن الطّفل تساعدهم على تحديد هويّته أو مكانه، وليس بالضّرورة أن يكون الولد نفسه من أفصح عنها، فقد يكون أحد الأقرباء أو الأصدقاء عن غير قصد قد وضع له صورة مثلاً على الشّبكة أو ذكّره بموعد ما أو ناداه باسمه.
- اختيار اسم مستخدم ومعلومات وهميّة، وكلمة سرّ غير كاشفة عن أيّ معلومات شخصيّة تخصّ الطّفل لا سيّما خلال التّدوين، وفي منتديات المناقشة والشّبكات الاجتماعيّة، وغرف الدّردشة...

• مخاطر متعلّقة بجرائم المعلوماتيّة:

تعمل مجموعات من قراصنة الإنترنت على اقتحام أجهزة الكمبيوتر للشّركات والمؤسّسات الحكوميّة من أجل تدمير المعلومات وتسريبها، كما تقوم أيضًا بسرقة وقرصنة البرامج الّتي لها حقوق ملكيّة، وحقوق النّسخ، ناهيك عن عمليّات الغشّ والاحتيال والخداع والنصب وكلّها مرادفات لجرائم معروفة منذ القدم.

وبفضل الإنترنت أخذت هذه الجرائم منحًى جديدًا، فأصبحت أكثر احترافيّة وازداد عدد ضحاياها. ومن أهم ما يميّز هذه النّوعية من الجرائم أنّها أصبحت عابرة للقارات ولا تعرف حدودًا، فقد تقع في فخ نصبه أحد المحتالين في دولة أخرى، وسوف يكون من الصّعب حينها أن تحصّل حقّك منه أو حتّى أن تقاضيه.
والأطفال هم الأكثر عرضة للسّقوط ضحايا هذه الأفعال. وفي بعض الأحيان يعمد هؤلاء القراصنة إلى تجنيد أو استغلال الأطفال للقيام بهذه المهام.

من أشهر أنواع جرائم النّصب والاحتيال والخدع الّتي تنتشر على الإنترنت ويجب أن تحذروا منها نذكر:

- **البريد الإلكتروني المزوّرscam :** هو بريد يُرسل إليكم من طريق شخص لا تعرفونه في الغالب. تكون هويّة المرسل مزوّرة بحيث يظهر أنّ مرسل الرّسالة هو شخص ذو منصب معيّن (كمدير شركة أو بنك أو من فريق صيانة موقع معروف مثل yahoo، hotmail، facebook)، لذا يكون من الصّعب معرفة الشّخص الّذي قام بإرساله، ويطلب إلى المستخدم معلومات عن حسابه متذرّعا بحجّة ما، أو حالة طارئة فيُخدع المستخدم بذلك ويستجيب لطلبه.
إنّ الـ Scam طريقة مشهورة للقيام بالاحتيال عبر الإنترنت. وأصبح شائعا لأنّ أشخاصا سذجا يستجيبون له، تكلفته زهيدة، سهل الإنشاء، ويصعب تعقّب فاعله. وهناك الكثير من عروض الـ Scam وما هي إلّا

عمليّات احتيال، مثلاً: يتمّ إقناع شخص ما بأنّه ربح مبلغًا في القرعة، أو ربح تذكرة سفر، ثمّ يطلب إليه إرسال مبلغ من المال ليصار لاحقًا إلى تحويل الجائزة الّتي ربحها.

- **تزوير صفحات المواقع:** بحيث تظهر صفحة الموقع مطابقة للصّفحة الرّسميّة لموقع آخر، وإذا كانت هذه الصّفحة، على سبيل المثال، تزويرًا لموقع حسّاس (موقع إلكتروني لمصرف)، فإنّ المستخدم المخدوع قد يُدخل بيانات حسابه فيها ما يؤدّي إلى سرقتها. لذا تذكّروا جيّدًا ألّا تستخدموا البريد الإلكتروني لمعالجة معاملات مصرفيّة وحسابات ماليّة.

- **سرقة الهويّة وخدع المعاملات الماليّة:** يتمّ ذلك عن طريق رسالة بريد إلكتروني أو رسائل نصّيّة قصيرة SMS على الهواتف النّقالة، حيث يعد الطّرف الخادع الطّرف المخدوع بنسبة كبيرة من ثروة وهميّة مقدّرة بالملايين، شرط أن يجري المستخدم المخدوع أوّلًا بعض التّرتيبات لاستلامها. ومن بعض الأمثلة: تصلكم رسالة تخبركم بأنّكم فزتم بجائزة ماليّة ضخمة في برنامج للجوائز، وعليكم أن ترسلوا مبلغًا من المال من أجل معاملات مصرفيّة أو الاتصال برقم هاتفيّ، أو شخص يطلب إليكم مساعدته لكي يحوّل إلى رصيدكم جزءًا من رصيد أحد الأشخاص المتوفّين، ويغريكم بالحصول على نسبة من المال ثمّ يطلب إليكم الإفصاح عن بعض معلوماتكم الشّخصيّة كرقم حسابكم أو رقم بطاقة الائتمان لكي يقوم بعمليّة التحويل.
اذا انخدعتم بهذه الرّسائل ينتهي بكم المطاف إلى الوقوع في جريمة معلوماتيّة تكونون ضحيّتها، إمّا بسرقة أموالكم أو حساباتكم أو معلوماتكم الشّخصيّة، أو باستخدام معلوماتكم الشّخصيّة لارتكاب جرائم من طريق هؤلاء المجرمين، وهذا ما يسمى بسرقة الهويّة أو Identity Theft.
لا تستهينوا بالأمر فهناك العديد من العصابات الّتي تعرف بعصابات الجرائم المنظّمة على الإنترنت، تمامًا كما هم على أرض الواقع. ولديهم طرق وأساليب ماكرة للإيقاع بضحاياهم، لذا لا تنساقوا أبدًا وراء هذه الرّسائل الّتي تحوي أيّ مضمون من المضامين السّابقة، وفكّروا جيّدًا قبل أن تتفاعلوا مع أيّ شخص واسألوا أنفسكم: «ما الّذي سوف يجعل شخصًا لا يعرفني أن يختارني بشكل عشوائي ليتقاسم معي مبلغًا من المال؟ أو ليخبرني أنّني ربحت جائزة ماليّة، وأنا لم أشترك في أيّ مسابقة أو سحب؟».

- **اللّوحات الإعلانيّة Bulletin Boards والرّسائل المنبثقة pop-ups الملغومة:** وهي تطلب إلى المستخدم التّسجيل والنّقر على إعلاناتها بهدف تشغيل برنامج تعرض الإعلانات على جهازه وذلك مقابل الحصول على مبلغ معيّن، أو التّسجيل في موقع وإرسال رابط دعائي له إلى مستخدمين آخرين ليزيد من نسبة ربحه، كما تقوم بإغرائه بفرص عمل، تأشيرات دخول لبلد معيّن، تذاكر سفر، .... والهدف من هذه الخدع هو انتزاع المعلومات الشخصيّة واستغلالها، أو عمليّات تسويق دعائيّة مجانيّة لهذه المواقع من دون مقابل مادي للمخدوع، أو تنزيل الفيروسات وملفّات التّجسّس على الحاسوب بهدف استغلال البيانات الشّخصيّة في عمليّات احتيال ونصب. وكثيرًا ما تستخدم عناوين مزيّفة وخادعة لروابط ومواقع غير أخلاقيّة مثل مواقع الاستغلال الجنسي للأطفال، والمواقع المشجّعة على تعاطي المخدرات وترويجها وغيرها.
- **الخداع التّضامني Hoax** : أي عندما يقوم بعض المستخدمين الّذين يقعون ضحايا لإحدى أنواع احتيال الإنترنت بالتّسويق لهذه الخدع وتأكيد صحّتها ومصداقيتها (سواءً أكانوا يعلمون حقيقتها أم يجهلونها)، ما

يؤدي إلى وقوع المزيد من الضّحايا فيها. مثل: اكتشاف دواء لمعالجة السّرطان أو وسائل للوقاية منه، أو المساعدة على الإبلاغ عن طفل مفقود....

بعض النّصائح لتفادي الاحتيال والخداع على الإنترنت:

- لا تفتحوا رسائل البريد الإلكتروني المرسلة من شخص لا تعرفونه، أو اللّوحات الإعلانيّة، أو الرّسائل المنبثقة Pop-Up لا سيّما إذا كانت تعدكم بالمال، أو الرّبح السّريع، أو الصّحّة الجيّدة، أو تأشيرة دخول لبلد معيّن، أو تذاكر سفر، أو فرص عمل..•
- استخدموا البرامج المضادة للفيروسات، برامج مكافحة التّجسس، وجدار الحماية firewall، وحدّثوا كلًّا منها بشكل منتظم.
- لا تردّوا على أيّ بريد إلكتروني، ورسائل منبثقة pop-ups، ولوحات إعلانيّة، وملف مرفق أو روابط links يطلب إليكم إعطاء معلومات شخصيّة أو ماليّة.

• مخاطر تبادل الملفّات FILE-SHARING:

إنّ شبكات النّد للنّد peer-to-peer network أو برامج تبادل الملفّات تسمح بتبادلها مع الآخرين عبر الشّبكة، ويستطيع أعضاؤها رؤية البيانات والموارد المخزّنة على أيّ من الأجهزة المتّصلة على الشّبكة والاستفادة منها. هل فكّرتم بما يمكن أن يجده الأطفال على الأقراص الصّلبة hard disk للآخرين؟

من بعض مخاطر هذه البرامج:

١. **التعرّض لمواد إباحيّة:** إنّ العديد من هذه البرامج يعرّض الأطفال إلى إمكانيّة الوصول إلى ملفّات إباحيّة فاحشة مثلًا: من خلال البحث عن ملفات موسيقى تحمل الكلمات الأساسيّة نفسها لمواد غير لائقة أو من طريق التّفتيش بملفات الآخرين والّتي قد تحوي ملفّات فيديو أو صورًا إباحيّة.
٢. **خطر المتحرّشين بالأطفال Pedophiles :** يعتبر المتحرّشون بالأطفال هذه الشّبكات من أفضل الوسائل للإيقاع بالضّحايا، ويستخدمون أسماء وعناوين خادعة خلال إرسالهم البريد المزعج، والإعلانات لجذب الأطفال والمراهقين، مثل: عناوين برامج للأطفال والمراهقين أو أسماء أبطال رسوم متحرّكة.
٣. **الفيروسات والبرمجيّات الخبيثة:** يشكّل استخدام الشّبكات الإجتماعيّة والبرامج خطرًا على الأجهزة بسبب قدرة الفيروسات والبرامج الخبيثة على الانتشار من جهاز إلى آخر عبر الشّبكة، والانتقال إلى جهازكم الخاص، لذا لا تنسوا تزويد الحاسوب ببرامج مضادة للفيروسات والبرامج الخبيثة والمتجسّسة، واعملوا على تحديثها بشكل دائم.
٤. **انتهاك الخصوصيّة:** تحوي بعض البرامج ثغرات تقنيّة قد تعرّض بيانات جهازك لخطر الاختراق لاسيما وأنّ ملفّاتك وبياناتك تصبح مكشوفة لجميع مستخدمي الشّبكة، وعرضة للاستغلال. مثل رقم بطاقة الائتمان، كلمة السرّ لحسابات معيّنة أو ملفات شخصيّة.

٥. **التّعدّي على حقوق الطّبع والنّشر:** إنّ تكنولوجيا النّد للنّد تجعل تبادل جميع أنواع المعلومات ممكنًا، وبعض هذه المعلومات محميّة بحقوق الطّبع والنّشر ما يعني أنّ هناك حاجة لطلب إذن من صاحب حقوق الطّبع

والنّشر قبل إتاحتها للمستخدمين الآخرين. مثل الموسيقى الشّعبيّة، الأفلام، الألعاب والبرامج. ويمكن أن يؤدّي التّعدّي على حقوق النّسخ والنّشر إلى فرض غرامات وعقوبات جنائيّة في حال رفع بعض أصحاب حقوق التّأليف والنّشر دعاوى مدنيّة ضدّ الفاعلين. لذلك على الأطفال أن يفهموا أنّهم لا يملكون الحقّ في إعادة نشر أو توزيع المواد الّتي تملك حقوق الطّبع والنّشر من دون إذن. وهذا يشمل تقديم نسخ من هذه المواد للأصدقاء، أمّا في حال استخدام بعض النّصوص من المواقع في مشاريع مدرسيّة، فعليهم أن يستشهدوا بالمصادر الصّحيحة.

بعض النّصائح لتجنّب مخاطر تبادل الملفّات:

- **اختيار البرنامج المناسب:** مع الأخذ بعين الاعتبار مستوى الرّقابة الأبويّة، ونوعيّة الحماية، وفعاليّة تصفية المحتويات الّتي يؤمّنها البرنامج.
- **المناقشة:** التّكلّم مع الأطفال عن أخلاقيّات الإنترنت في قضايا مثل حقوق النّشر، وعن الخصوصيّة في قضايا الإفصاح عن معلومات شخصيّة.
- **المراقبة:** استخدام برامج رصد monitoring لتتبّع أنشطة الأطفال على الإنترنت.

• المقامرة على الإنترنت:

هناك العديد من مواقع المقامرة على الإنترنت، ويمكن لأيّ شخص لديه بطاقة ائتمان تحت تصرّفه أن يشارك بالمقامرة. علينا أن ندرك أن مشاركة القاصرين في المقامرة غير قانونيّة، لذا لا تعطوا أطفالكم رقم الحساب المصرفي أو رقم بطاقة الائتمان. ومن الأفضل أن تدقّقوا من حين إلى آخر في مدفوعات بطاقة الائتمان للتّأكّد من أنّه لم يتمّ صرف مبالغ لمدفوعات غير عاديّة.

• خطر البرمجيّات الماكرة أو الخبيثة MALWARE:

هي برامج مخصّصة للتّسلّل إلى نظام الحاسوب، لتدميره أو تعطيل أدائه من دون رضى المالك. ما إن يتمّ تثبيت البرمجيّة الخبيثة فإنّه من الصّعب جدًّا إزالتها. ويتراوح أذاها بحسب درجة البرمجيّة من إزعاج بسيط (بعض النّوافذ الإعلانيّة غير المرغوب بها خلال عمل المستخدم على الحاسوب سواء أكان متّصلاً بالشّبكة أم غير متّصل) إلى أذى غير قابل للإصلاح يتطلّب إعادة تهيئة (format) القرص الصّلب على سبيل المثال.

من الأمثلة على البرمجيّات الخبيثة:

١. **حصان طروادة أو Trojan Horse:**
برنامج خادع ويبدو كأنّه مفيد، ولكنّه بالحقيقة يهدّد أمن الكمبيوتر وبيانته ويتسبّب بالأضرار.
ظهر مؤخّرًا حصان طروادة على شكل بريد إلكتروني يتضمّن مرفقات، تمّ الإدّعاء بأنها تحديثات أمن security updates من مايكروسوفت، وتبيّن أنها فيروسات تحاول تعطيل برامج مكافحة الفيروسات وجدران الحماية.

كيفيّة الإصابة به: يمكن أن يصيب حصان طروادة Trojan الحاسوب بطرق عدّة نذكر منها:

- **برامج المحادثة:** مثل Yahoo، MSN، ICQ، Microsoft chat وغيرها، لذا لا تستقبلوا أيّ ملف خصوصًا إذا كان امتداده exe إلا من شخص تثقون به تمام الثّقة.
- **البريد الإلكتروني:** لا تفتحوا أيّة رسائل تكون من شخص أو من جهة غير معروفة بل احذفوها فورا.
- **المواقع المشبوهة:** قد يؤدّي تحميل بعض الملفّات إلى إصابة حواسيبكم بأحصنة طروادة.
- **المنتديات:forums** الّتي تُفَعِّل خاصيّة html إذ قد يأتي حاقد على المنتدى ويزرع الرّمز code في ردّ على موضوع أو في موضوع جديد.

كيفيّة التّخلّص من التّروجان والوقاية منه:

- من طريق برامج الحماية.

لا تستطيع برامج الحماية في بعض الأحيان أن تتخلّص منه إذ قد يحذف معه ملفًا مهمّا من ملفّات النّظام، في هذه الحال أنتم بحاجة إلى مساعدة تقني اختصاصي في المعلوماتيّة يقوم بحذفه من طريق ال (Disk Operating System DOS).

٢. ما هي الدّيدان Worms:

هي برنامج ضارّ يقوم بمضاعفة نفسه من خلال الإنترنت وينتقل من جهاز إلى آخر. وهذا البرنامج يقوم باستخدام مصادر الكمبيوتر وإغلاقه. لذا فإنّ إغلاق الكمبيوتر فجأة يدل على وجود نوع من الدّيدان فيه.

٣. ما هو الفيروس Virus:

هو أيضًا برنامج خبيث يقوم بإدراج نفسه داخل ملفّ، ويهدف إلى تعطيل العمل في الكمبيوتر. تعتبر الدّيدان نوعًا من الفيروسات إلا أنّها لا تستطيع إدراج نفسها في ملفّ، ولا تستطيع الفيروسات بالمقابل مضاعفة.

كيفيّة الوقاية والتّصدّي للدّيدان والفيروسات:

- لا تبقوا وحدات تخزين المعلومات Floppy في الدّرايف، أثناء بدء تشغيل الكمبيوتر، أو بعد إغلاقه، لأنّ الفرصة تكون أكبر لانتشار الفيروسات.
- أجروا مسحًا Scan لوحدات تخزين المعلومات قبل فتح الملفّات فيه، لأنّ هذه الطّريقة تسمح بالتقاط الفيروسات قبل انتشارها في الكمبيوتر.
- امسحوا مختلف الملفّات أو البرامج الّتي تريدون تنزيلها من الشّبكة قبل فتحها أو تشغيلها.
- ألغوا الرّسائل الإلكترونيّة المتطفّلة Spam مباشرة لأنّها قد تحمل معها الفيروسات.
- تجنّبوا البرامج المنسوخة، ولا يغرّكم سعرها المنخفض، لأنّها قد تكون ملوّثة بالفيروسات، ناهيكم عن تجاوز أصحابها القراصنة لقانون الملكيّة الفكريّة.
- تأكّدوا بأنّ برنامج مقاومة الاختراق، معدّ بطريقة مناسبة، بحيث يصدّ ملفّات التّجسّس الّتي قد تنقل

إلى المخترقين معلومات عن حواسيبكم الشّخصيّة، وتجعلها بالتّالي عرضة للفيروسات والتّجسّس.

- اجعلوا برنامج مقاومة الفيروسات على أهبة الاستعداد للتّصدّي لها، من خلال تحديثه update باستمرار.
- تتبّعوا أخبار الفيروسات للاطلاع على كلّ جديد.
- في حال تعرّض جهازكم لفيروس، لا تقلقوا، قوموا بتشغيل برنامج المقاومة، واتبعوا التّعليمات لإزالة الفيروس حتّى النّهاية.

٤. **البرمجيات الدعائيّة Adware:**

يتوافر العديد من البرامج المجانيّة على شبكة الإنترنت، وعند تحميلها يتمّ تنزيل البرمجيات الدعائيّة معها، حيث إنّ اتفاقيّة قبول هذه البرامج تنصّ على قبولكم بوجود البرمجيات الدعائيّة، ولكن بشكل مبهم، وهذه هي ضريبة البرامج المجانيّة.

وتقوم هذه البرامج بعرض الإعلانات بصورة مستمرّة حتّى لو لم تكونوا قد قمتم بتشغيل البرنامج الأصلي الّذي تمّ تنصيب البرمجيات الدعائيّة معه.

لا تتوقّف حدود البرمجيات الدعائيّة عند هذا الحدّ بل تتعقّب الصّفحات الّتي تزورونها لمعرفة اهتماماتكم وهواياتكم لتعرض لكم الإعلانات الّتي تتناسب مع اهتماماتكم.

كذلك تقوم البرمجيات الدعائيّة بالحصول على معلومات عنكم من جهازكم كمعرفة بريدكم الإلكتروني وبالتّالي إرسال الإعلانات إليه، أو إرسال بريدكم الإلكتروني إلى الجهات الّتي سوف تستفيد منها.

كما يمكن للـ Adware أن يقوم بتغيير الصّفحة الرّئيسة لمستعرض الإنترنت، ولن ينفع تعديلك لها لأنّها سوف تتغيّر باستمرار.

كيفية التّخلّص من البرمجيات الدعائيّة:

الهدف العامّ للـ Adware هو الإعلانات فلماذا نقوم بإزالتها؟ الجواب بسيط بإزالة البرمجيات الدعائيّة لن تحتاجوا إلى إغلاق النّوافذ الإعلانيّة كلّما أردتم الذّهاب إلى صفحة ما، وبذلك توفّر عليكم الوقت.

طبعًا صانعو البرمجيات الدعائيّة يجعلونه صعب التّعقّب، وفي بعض الأحيان لا تستطيعون إزالته بسهولة. لذلك يجب أن يكون لديكم برنامجًا خاصًّا بالتّصدّي للأدوير Anti-Adware ويجب تحديثه باستمرار للتّأكّد من قدرته على مواجهة أحدث أنواع البرمجيات الدعائيّة، وإذا أردتم أن تستمر برامجكم المجانية بالعمل فعليكم عدم إزالة كلّ أنواع البرمجيات الدعائيّة.

٥. **الرّسائل غير المرغوب فيها Spam:**

ال Spam هو بريد يُرسل إليك من طريق شخص غريب، هويّته مزوّرة، لذا يكون من الصّعب معرفته.

وهو طريقة مشهورة للقيام بالاحتيال عبر الإنترنت من خلال حيل الثّراء السّريع المتعدّد، وأحيانًا قد يُطلب إلى المستخدم زيارة مواقع على الويب تتنافى مع الأخلاق.

تكلفة هذه الرّسائل زهيدة، سهل إنشاؤها، وصعب تعقّب فاعلها. كمّا أنّ هناك الكثير من عروض الـ Spam ما هي إلا عمليّات احتيال وإن لم تكن كلّها كذلك.

أصبح الـ Spam شائعًا لأنّ الأمر لايكلّف أصحاب هذا النّوع من البريد محاولات كثيرة فالعديد من الأشخاص ينخدعون به بسهولة، وهو يحقّق مكاسب كثيرة.
والجدير بالذّكر أنّ الـ Spam يعوّق صناديق البريد الإلكتروني وملقّمي البريد ما يؤدّي إلى بطء وصول البريد أو أحيانًا عدم وصوله، ويجبر مزوّدي الخدمة على شراء المزيد من عروض النّطاق حتّى يتمكّنوا من إرسال البريد الرّائد.

٦. ما هي البرمجيات التجسّسيّة Spyware:

عندما نتكلم عن عدم وجود الخصوصيّة في الشّبكة العنكبوتيّة فنحن نقصد البرمجيات التجسّسيّة.
فالبرمجيات التجسّسيّة عبارة عن برنامج تجسّسي يتعقّب تحرّكاتكم على الشّبكة العنكبوتيّة، ويعرف عنكم معلومات كثيرة من دون علمكم.
وهذه المعلومات لا تقتصر على بريدكم الإلكتروني فحسب (مثلما يفعل البرمجيات الدعائيّة) بل تتعدّاها لتصل إلى كلمات المرور الخاصّة بكم، حتّى أنّه قد يحصل على رقم بطاقتكم الإئتمانيّة إذا كنتم تستخدمونها للشّراء عبر الإنترنت.
فالـ Spyware شبيه بالبرمجيات الدعائيّة إلّا أنّه أكثر خطرًا، في حين أنّ الهدف العامّ للـ Adware هو الإعلانات فإن الهدف من البرمجيات التجسّسيّة سرقة بياناتكم السّرّيّة، وإن اقتضى الأمر سرقة أموالكم.
وتذكّروا أنّ الشّخص الّذي يتجسّس عليكم يمكنه معرفة كلّ ما يدور بجهازكم وكأنّه جالس معكم.

كيفية الإصابة بالبرمجيات التجسّسيّة:

تنتشر هذه البرامج بثلاث طرق رئيسة:

- الطّريقة الأولى تنتج من قيام المستخدم باتخاذ خطوة ما تتسبّب بإطلاق الكود وتنفيذه من دون علمه كما هي الحال مع الفيروسات، وقد تكون تلك الخطوة فتح رسالة بريد إلكتروني، أو ملفّ مرفق برسائل البريد الإلكتروني، أو مجلّدات تجري المشاركة فيها عبر الشّبكات (إنترنت أو شبكة داخليّة)، وعبر برامج المراسلة الفوريّة، أو من طريق تثبيت بعض التّطبيقات المجانيّة أو برامج تبادل الملفّات.
- الطّريقة الثّانية تعتمد على الهندسة الاجتماعيّة حيث إنّها تستخدم أساليب التّحايل لجذب المستخدم للنّقر على وصلة link أو فتح ملفّ مرفق بالبريد أو تثبيت برنامج مجاني.
- الطّريقة الثّالثة وهي تعتبر أخطر طريقة ولا تتطلّب من المستخدم أيّ إجراء عدا تصفّح الإنترنت بطريقة عاديّة وتسمى drive-by downloading أي بمجرّد زيارة موقع، أو مشاهدة إعلانات Pop-up مجهّزة لنشر تلك البرامج التّجسّسيّة تحصل الإصابة بالكود الضّار.

كيفيّة التّخلّص من البرمجيات التجسّسيّة:

يتمّ التّخلّص منها من طريق البرامج المضادة للبرمجيات التجسّسيّة Anti-Spyware.

قواعد للأطفال من أجل إبحار آمن على الشّبكة:



١. الحفاظ على الخصوصيّة:

كلّ ما ينشر على الإنترنت يصبح بمتناول الجميع ولا يمكن استرداده، فمن السّهل استغلاله للإساءة إليّ أو لتشويهه من قبل الغرباء، لذلك:

- أنا أرفض إعطاء أيّ شخص على الإنترنت معلومات شخصيّة عنّي أو عن أهلي (كلمة السّرّ، اسمي الكامل، بريدي الإلكتروني، عنوان المنزل، صور، رقم تلفون، عنوان مدرستي، مكان عمل أهلي، رقم بطاقة الائتمان credit card).
- أنا أستشير دائمًا شخصًا راشدًا أثق به في حال الاضطرار إلى إعطاء معلومات شخصيّة، وأختار اسم مستخدم وكلمة مرور لا يكشفان عن أيّة معلومات شخصيّة تخصّني.
- أنا أستفيد من أدوات الخصوصيّة Privacy Settings للحفاظ على خصوصيّة معلومات ومحتويات لا أريد أن أشاركها مع الجميع.

٢. تجنّب محادثة الغرباء ولقائهم:

ليس بالضّرورة أن يكون من نتحدّث إليه على الإنترنت الشّخصيّة الّتي يدّعيها، فقد يكون منتحلًا شخصيّة أخرى بصورة مزيّفة، وعمر مزيف، فالغريب على شبكة الإنترنت قد يكون متحرّشًا أو من قراصنة الأطفال، لذلك:

- أنا لن أتحدّث إلى الغرباء على الإنترنت لأنّه من السّهل انتحال شخصيّة غير حقيقيّة بغرض الإساءة إليّ.
- أنا أرفض مقابلة أيّ شخص غريب تعرّفت إليه على شبكة الإنترنت من دون استشارة أهلي أو شخص راشد أثق به. وفي حال موافقتهم، لن أقابله وحدي بل بوجودهم أو بوجود شخص راشد معي.
- أنا أخبر دائمًا شخصًا راشدًا أثق به عن أيّ شيء أو أيّ شخص يزعجني على الإنترنت.

٣. المحافظة على سمعة رقميّة جيّدة:



أنا أحترم الآخرين ولا أسيء إليهم خلال استعمالي الشّبكة فما يصحّ في حياتي الواقعيّة يصحّ في عالمي الرّقمي أيضًا، لذا:

- لن أكتب أيّ تعليق يسيء إلى أحد أو يجرح مشاعره.
- لن أنشر أشياء على الإنترنت تخصّ الآخرين من دون موافقتهم أو علمهم بالأمر (كالصّور، رقم الهاتف، عنوان البريد الإلكتروني...).
- لن أخرق قوانين الملكيّة الفكريّة وقواعد الآداب العامّة المتعارف عليها اجتماعيًّا. مثل: نسخ موسيقى، وألعاب، وبرامج. فهذا العمل يعتبر سرقة ويعرّض مرتكبه للملاحقة القانونيّة.

٤. التّأكّد من صحّة المعلومات:

يمكن لأيّ شخص أن يكتب ما يشاء على الشّبكة من دون مراقبة، من هنا فإنّ المعلومات الموجودة على الشّبكة ليست كلّها صحيحة، لذلك:

- أنا أراجع دائمًا المعلومات الّتي أحصل عليها من الشّبكة وأتأكّد من دقّتها، لأنّها ليست دائمًا صحيحة ودقيقة، وذلك من طريق الاستناد إلى أكثر من مرجع ومصدر.
- أنا أطلب من شخص راشد أثق به أن يتأكّد من صحّتها.



٥. التّوازن في استخدام الوقت:



أنا أعرف كيف أوازن بين الوقت الّذي أقضيه على الإنترنت وقيامي بأنشطة أخرى مثل الرّياضة، إتمام واجباتي المنزليّة والمدرسيّة، تمضية وقت مع الأصدقاء والعائلة...

٦. حماية الحاسوب الشّخصي والمعلومات الشّخصيّة:

باتخاذ أربع خطوات أساسيّة، يمكنني حماية الحاسوب الشّخصي من الكثير من البرمجيّات الخبيثة الّتي قد يتعرّض لها، لذا:

- أنا أستخدم البرمجيّات المضادة للفيروسات وأحدّثها دوريًّا.

- أنا أتجاهل الرّسائل البريديّة المزعجة أو المجهولة المصدر وأحذفها، وأعلم أنّ كلّ رسالة تحوي عرضًا مغريًا هي مزيّفة.
- أنا لن أجيب عن أيّة رسالة إلكترونيّة يطلب إليّ فيها إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة.
- أنا أحصّن كلمة السرّ باستخدام ثمانية أرقام على الأقلّ تجمع ما بين الحروف والأرقام والرموز، وأقوم بتغييرها بشكل دوريّ.
- أنا لا أحمّل الملفّات (download) أو أنقر على الوصلات links) أو الملحقات (attachmentss) إلاّ في حال كنت أثق تمامًا بالمصدر.
- أنا لا أفتح أو أردّ على أيّ بريد إلكتروني أو رسالة مرسلة من شخص أو مصدر لا أعرفه.

٧. الإبلاغ عن الإساءات:

خلال استخدامي الشّبكة، قد أتلقّى رسائل مزعجة أو رسائل تهديد تجعلني أشعر بعدم الارتياح، في هذه الحال:

- أنا أعلم أنّه ليس خطئي إن تلقيت مثل هذه الرّسائل، ومن حقّي أن لا أردّ عليها.
- أنا أخبر على الفور أهلي أو أيّ شخص راشد أثق به.



قواعد تساعد الأهل على تأمين بيئة أكثر أمانًا للأطفال على الشّبكة:

الشّبكة المعلوماتيّة ليست آمنة في كلّ الأحوال، وخطرها سيكون أكبر بالنّسبة إلى الأطفال منه بالنّسبة إلى الكبار، لأنّهم يتعرفون إليها ويدخلونها بحماسة وبصفة شبه يوميّة ولا يجدون من يرشدهم إلى تلك المخاطر. ومنع الأطفال من استخدام الإنترنت ليس الطّريق الأمثل لإبعادهم عن هذه المخاطر، وأفضل أسلوب هو معرفة الخطوات الّتي يجب اتخاذها للإبحار على الشّبكة العنكبوتيّة بأمان.
ويحاول الآباء بشكل خاص حماية أطفالهم من المواقع الإباحيّة، أو من محاولة استغلالهم عبر غرف الدّردشة. وعلينا كمربّين وأهل أن نتحمّل مسؤوليّة حماية أطفالنا، وتأمين سلامتهم من طريق اتّباع ستّ قواعد ذكيّة عند استخدام «النّتّ». والطّريقة الأفضل أن نتّفق معهم على احترام هذه القواعد وتطبيقها في إطار ما نسميه «شرعة استخدام النّتّ». وكما يعرّضنا استخدام السّيّارة مثلًا إلى مخاطر عديدة إذا لم نحترم قواعد السّير، فالإبحار الآمن على الإنترنت يتطّلب ستّ قواعد بسيطة وذكيّة، وهي:

١. الحيطة والحذر:

علّموا أطفالكم بديهيّات أو أساسيّات سلامة استخدام الإنترنت:

- عدم إعطاء معلومات شخصيّة مثل الاسم، العمر، المدرسة، العنوان.
- عدم إرسال أو مشاركة الصّور مع غرباء وتأكّدوا من استخدامهم لأدوات الخصوصيّة Privacy Settings.
- الاحتفاظ بسرّيّة كلمات المرور Password.
- عدم التّحدّث إلى الغرباء في غرف الدّردشة، وعدم استقبال رسائل بريديّة E-Mails منهم أو فتحها.
- إخبار شخصٍ راشد فور الشّعور بعدم الارتياح.

حاولوا، ولو لمرّةٍ واحدة، أن تستخدموا مختلف أنواع محرّكات البحث مثل Google لتبحثوا عن اسمكم أو اسم أحد أفراد عائلتكم، حتمًا سوف تذهلون لما ستجدونه (أين وصل أولادكم بتجوالهم، وكم يعرفون عنكم على الشّبكة...)

٢. المراقبة والتّحكّم:

- استخدموا برمجيّات المراقبة الأبويّة (parental control) المتوافرة لمساعدتكم على تصفية المحتويات المضرّة، ومراقبة المواقع الّتي يزورها الأطفال ومعرفة ما يفعلونه.
  في حال كان أطفالكم دون الـ ١٢ سنة عليكم مرافقتهم في استخدامهم للإنترنت، أصرّوا على أن يكون لكم حقّ الدّخول إلى حساباتهم الإلكترونيّة، وعلب رسائلهم لكي تتأكّدوا من عدم تواصلهم مع الغرباء. أمّا في حال كان عمر أطفالكم فوق الـ١٢ سنة فشاركوهم عالمهم من دون رقابة بوليسيّة، علّموهم كيف يحمون أنفسهم ويثقون بحدسهم وذكائهم.
- ضعوا الحاسوب ولا سيّما وصلة الإنترنت في مكانٍ عامّ في المنزل وليس في غرفة نوم الأطفال.

- اتفقوا مع أولادكم على طبيعة المواقع المسموح زيارتها.
- اتفقوا مع أولادكم على وضع قواعد لاستخدام الإنترنت، وذلك من خلال تنظيم وقت استخدامهم للشّبكة والمدّة.
- توافقوا مع أطفالكم على مبادئ وقواعد التّحميل download: كالموسيقى المسموح بها، والأفلام المسموح بها، نوعيّة الألعاب الّتي يحمّلونها. اختاروها معهم، وتأكّدوا من أنّ برامج الألعاب تناسب عمرهم من حيث المضمون، واحذَروا الألعاب الّتي تتضمّن العنف والمشاهد الدّمويّة لأنّ لها تأثيرًا «سلبيًّا» في تكوين شخصيتهم وسلوكيّاتهم.

٣. أخلاقيّات الإنترنت:

علّموا أطفالكم أنّ ما يصحّ في حياتهم الواقعيّة يصحّ في عالمهم الرّقمي، لذا عليهم:

- أن يحافظوا على سمعة رقميّة جيّدة.
- ألّا ينشروا محتوًى أو صورًا محرجة للآخرين ومن دون علمهم أو موافقتهم.
- ألّا يخرقوا قوانين الملكيّة الفكريّة وقواعد الآداب العامّة المتعارف عليها اجتماعيًّا، وأن يستشهدوا بالمصادر بالشّكل الصّحيح.
- ألّا يقوموا بنشر أو تدوين أيّ تعليق مسيء للآخرين.
- ألّا ينضمّوا وألّا يشاركوا في تأييد المجموعات group invitation المسيئة للآخرين أو المسيئة للمعتقدات والأديان والّتي تروّج لأفكار وقضايا تتنافى مع الأخلاق والآداب مثل العنصريّة، العنف، الأفكار الشّيطانيّة، الإرهاب، السّاديّة، التّشجيع على تعاطي المخدّرات والانتحار، والسّحر والشّعوذة، وقتل النّفس...

٤. فتح باب الحوار والتّواصل:

أبقوا على قنوات الحوار والتّواصل مع أطفالكم مفتوحة، وتحدّثوا إليهم عن:

- مراكز اهتمامهم على الشّبكة، ونوعيّة عملهم، والمواقع الّتي يزورونها عادة.
- الأشخاص الّذين يتواصلون معهم في غرف الدّردشة والمراسل الفوري.
- ضغط الأقران، فسّروا لهم أنّه ليس بالضّرورة أن يكون كلّ ما يقوم به أصدقاؤهم صحيحًا.

لا تتصرّفوا بعقليّة القاضي، وتصدروا الأحكام بل اسألوا وكونوا مستعدين للإجابة عن بعض الأسئلة الّتي لا تتوقّعونها ولا تحبّونها، وحافظوا على حرّيّة النّقاش ومرونته.

٥. التّعامل مع الإساءة والإبلاغ عنها:

علّموا أطفالكم طريقة التّعامل الصّحيح مع الخطر المحتمل، لأنّ بعض الأشخاص على الشّبكة قد يكونون من أصحاب النّوايا السيّئة تجاههم، لذلك يجب قبل كل شيء إفهامهم أن:

- لا يثقوا في إفراط مديح الأشخاص الغرباء لهم وفي وعودهم لهم بالمال، والهدايا، والمتعة والحنان...
- لا يجيبوا عن الأسئلة المتعلّقة بالبنية الجسديّة (القامة، الوزن، لون العينين، السّنّ...).
- يعلّموكم بمجرّد شعورهم بأنّ هناك شيئًا مريبًا يحصل.

- يستخدموا الإنترنت بشكل سليم، فسلامتهم على الإنترنت لن توقعهم في مشاكل كحرمانهم من استعمال الحاسوب.

٦. حماية الحاسوب الشّخصيّ:

تأكّدوا من استخدام برامج مكافحة الفيروسات وبرامج الحماية الشّخصيّة مثل برامج جدران النّار (firewall) الموجودة في الحاسوب وتحديثها بشكل دوريّ...(لمعلومات أكثر حول الموضوع راجعوا فقرة المعلومات التّقنيّة).

تقنيات الحوار والتّواصل الفعّال مع الأطفال:

يشغل موضوع الخلاف بين الأهل والأبناء اليوم حيّزًا مهمًّا في القضايا الاجتماعيّة المعاصرة، خصوصًا وأنّنا نعيش في عصر يتميّز بالتّحدّيات الكبيرة والتّطورات السّريعة. ويعتبر التّواصل الجيّد والفعّال مفتاحًا لبناء العلاقة الجيّدة والثّقة بالنّفس، والاحترام المتبادل بين الأهل والأطفال، وهو بحدّ ذاته مهارة مهمّة يجب أن يكتسبها الأهل بغية تجنّب الصّراعات، ولبناء علاقات إيجابيّة مع أطفالهم.

من المبادئ الأساسيّة للتّواصل الجيّد نذكر ما يأتي:

الإصغاء الجيّد:

- أظهروا لأطفالكم أنّكم مهتمون بكلّ كلمة يقولونها. وعندما يريدون أن يتحاوروا معكم أظهروا لهم اهتمامكم مثلًا: قوموا بإطفاء التّلفاز، أو ضعوا الصّحيفة جانبًا، أو تجنّبوا الرّدّ على مكالمات هاتفيّة. فهذا الفعل يشجّعهم أن يفتحوا قلوبهم لكم، ويبنوا ثقة واحترامًا متبادلاً فيما بينكم، ويجعلهم يدركون بأنّهم مهمّون بنظركم.
- استمعوا إليهم باهتمام وأدب، فلا تقاطعوهم عندما يحاولون إخباركم قصّتهم. فتهذيبكم ولطفكم معهم يساعدهم على بناء ثقتهم بأنفسهم، وعلى احترام الآخرين، ويجعلهم يشعرون بأنّكم أفضل صديق لهم.
- اطرحوا عليهم بعض الأسئلة للاستفسار عن شيء قالوه، وذلك ليتأكّدوا أنّكم تستمعون إليهم، ولا تكثروا منها كي لا يشعروا أنّكم تحقّقون معهم.

تجنّبوا الإحراج:

- حافظوا على خصوصيّة النّقاش بينكم وبين أطفالكم، ولا تتناقشوا معهم بأيّ موضوع أمام الآخرين، لأنّ هذا الفعل يسبّب لهم الإحراج ويؤدّي بهم إلى مزيد من الخجل والانطواء، فالتّواصل الفعّال يتمّ عندما تكونون وحدكم مع أطفالكم بمنأى عن الآخرين.
- لا تنتقدوا تصرّفات أطفالكم، ولا تسخروا منهم أو تطلقوا عليهم ألقابًا فهذا ما يشعرهم بالخجل، والحقد، والعدائيّة، ويفقدهم ثقتهم بأنفسهم وبكم.

الهدوء وتفادي الغضب:

- الغضب وباء معد، انتظروا أن يفرّغ أطفالكم غضبهم، وينتهوا من التّعبير عن مشاعرهم حتّى تعبّروا أنتم عن رأيكم بهدوء واستيعاب.
- بعد أن يهدأ أطفالكم فسّروا لهم سبب عدم رضاكم عن تصرّف معيّن قاموا به، واشرحوا لهم عواقب هذا التّصرّف، وأخيرًا ضعوا قواعد وتعليمات حتّى يتبعوها من دون أن توجّهوا إليهم الانتقادات والاتّهامات.
- في حال كنتم تشعرون بالاستياء والغضب الشّديد جرّاء تصرّف ما قام به أطفالكم، انتظروا حتّى تهدأوا قبل أن تتكلّموا معهم، لأنّه لا يمكنكم أن تكونوا موضوعيّين في حالتكم هذه.
- تكلّموا بلطف وهدوء مع أطفالكم لأنّ هذا ما يكسبكم صداقتهم وثقتهم بكم، وهو أمر أساسيّ للحفاظ على حوار إيجابيّ وفعّال. وتفادوا الصّراخ والغضب لأنّه يؤجّج الخصام والصّراع والعداء بينكم.

المواقف الإيجابيّة:

- خذوا موقفًا إيجابيًّا حيال الأنشطة الّتي يقوم بها أطفالكم، وشاركوهم بها، وادخلوا عالمهم، وتعرّفوا إلى مراكز اهتمامهم، واقضوا معهم الوقت الكافي، فهذه الأمور تساعد على تدعيم روابط العلاقة بينكم وبينهم.
- شجّعوهم على إنجازاتهم فالتّشجيع يساعدهم على السّلوك الحسن.
- كونوا لطفاء، وقدّموا إليهم الدّعم العاطفي والتّعزية عند الحاجة.
- لا تستخدموا العبارات الّتي تحطّ من معنوياتهم مثل: «هذا تصرّف أحمق»، «أنتم لا تعرفون شيئا»، «أنتم مجرّد أطفال لا تعرفون ما هو لصالحكم»...
- برهنوا لهم أنّكم تتقبّلونهم كما هم، بغضّ النّظر عن التّصرّف الّذي قاموا به، فالأطفال يعوّلون على الدّعم المعنوي.

الابتعاد عن أسلوب التّحقيق وإصدار الأحكام:

- لا تتصرّفوا بعقليّة القاضي، وتبدأوا بإصدار الأحكام وتوجيه الانتقادات لا سيّما وأنتم تصغون إلى أطفالكم.
- لا تنتقدوا تصرّفاتهم، ولا تسألوهم لمَ قاموا بهذا التّصرّف؟ بل اسألوهم: كيف حدث هذا الأمر؟
- واجهوا أطفالكم بالمعلومات الّتي تعرفونها في حال كنتم على علم بالمشكلة، وخفّفوا من أسلوب الوعظ والتّكلّم عن المثاليّات، وتوجيه العبارات الّتي تذكّرهم بأنّهم غير ناضجين وأنّكم راشدون، لأنّها لا تساعد على فتح قنوات الحوار، مثل: « افعلوا ما نقوله لكم»، « نحن نعرف ما هو الأفضل لكم»، «تكلّموا عندما ننهي كلامنا»...
- عندما يدرك الأطفال أنّهم على خطأ، ساعدوهم على وضع قواعد لتفادي ارتكابها مجدّدًا، فهذا الفعل يهيّئهم تدريجيّا لاتّخاذ القرارات المناسبة في المستقبل.
- لا تفرضوا أفكاركم على أطفالكم، بل تذكّروا دائمًا أنّهم ينتمون إلى جيل مختلف، ساعدوهم على التّخطيط للوصول إلى حلّ بكلّ محبة واستيعاب.

كلمات التّشجيع:

يحتاج الأطفال إلى التّشجيع، والشّعور بالحبّ والتّقدير، ولكنّ معظم الآباء يجدون أنّه من الأسهل عليهم توجيه انتقادات سلبيّة للأطفال عوضًا عن قيامهم بردود فعل إيجابيّة. لذلك ننصحكم باختيار بعض العبارات الآتية واستخدامها يوميًّا مع أطفالكم، وسوف تجدون أنّهم سيبدأون بإعارتكم المزيد من الاهتمام ويسعون جاهدين لإرضائكم، وعلى سبيل المثال يقول أحد الوالدين لأحد أبنائه:

هذا جيّد/ ممتاز/ رائع، فكرتك رائعة، أحبّك، يا لك من فتى مدهش، نجاح باهر، تقدّم ملحوظ، استمتعت بالحديث معك، كلامك في مكانه، كلامك منطقي، أحبّ الطّريقة الّتي _____، لاحظت أنّك_____، أنت تتحسّن أكثر فأكثر_____، لقد أثبت أنّك تستطيع أن تتحمّل مسؤوليّة_____، أنت رائع في_____، كم أنت جيّد في_____، لقد أمضيت وقتا رائعا برفقتك، لقد أبهرتني ب_____، أعجبتني_____، أنا فخور بك، أنا مسرور لأنّك...

كما يمكنكم استخدام بعض الحركات والإيماءات التّشجيعيّة مثل: التّربيت على الأكتاف، العناق، الابتسام، هزّ الرّأس، مداعبة الشّعر.

وأخيرًا نختم بهذه الأقوال الرّائعة للشّاعرة **Dorothy Law Nolte**:

- إذا كان الطّفل يعيش مع الانتقادات، فسوف يتعلّم الإدانة.
- إذا كان الطّفل يعيش مع الخصام، فسوف يتعلّم القتال.
- إذا كان الطّفل يعيش مع السّخرية، فسوف يتعلّم أن يكون خجولًا.
- إذا كان الطّفل يعيش في الخوف، فسوف يتعلّم أن يكون خائفًا.
- إذا كان الطّفل يعيش مع العار، فسوف يتعلّم أن يشعر بالذّنب.
- إذا كان الطّفل يعيش مع التّسامح، فسوف يتعلّم التّحلي بالصّبر.
- إذا كان الطّفل يعيش مع المديح، فسوف يتعلّم أن يقدّر.
- إذا كان الطّفل يعيش مع القبول، فسوف يتعلّم أن يحبّ.
- إذا كان الطّفل يعيش مع الصّدق، فسوف يتعلّم ما هي الحقيقة.
- إذا كان الطّفل يعيش مع الإنصاف، فسوف يتعلّم العدالة.
- إذا كان الطّفل يعيش في أمان وطمأنينة، فسوف يتعلّم أن يثق بنفسه وبالّذين حوله.
- إذا كان الطّفل يعيش مع الصّداقة والقبول، فسوف يتعلّم أن يجد الحب في العالم.

بعض المعلومات التّقنيّة:

كيفية تفعيل برامج المراقبة الأبويّة الموجودة في نظام التّشغيل WINDOWS®:

بإمكانكم الاستعانة ببرنامج المراقبة الأبويّة للمساعدة على إدارة استخدام أطفالكم للكمبيوتر. على سبيل المثال: يمكنكم وضع كلمة مرور للولوج إلى شبكة الإنترنت، وتحديد الوقت والمدّة الزّمنيّة للدّخول إلى جهاز الكمبيوتر، واختيار الألعاب والبرامج الّتي يمكن تشغيلها، والمواقع المسموح تصفّحها.

لكي تتمكّنوا من تشغيل المراقبة الأبويّة Parental Control، عليكم أن تقوموا بالخطوات الآتية:

١. اخلقوا حساب مستخدم **User Account** محدودًا **Limited** للأطفال الّذين تريدون إعداد المراقبة الأبويّة لهم **Parental Control**، لأنّه لا يمكنكم أن تطبّقوا هذا إلّا على حساب المستخدم المحدود **Limited Account**، ولخلق هذا الحساب اتبعوا التّعليمات الآتية:

- انقروا على زرّ **Start**، اختاروا **Control Panel**، وبعدها **User Accounts and Family Safety** لإنشاء حساب مستخدم.
- انقروا على إنشاء حساب جديد **Create a new account**.
- اطبعوا الاسم الّذي تريدون إعطاءه لحساب المستخدم، اختاروا نوع الحساب **Account type**، اختاروه محدّدًا للأطفال **limited** ثمّ انقروا على إنشاء الحساب **Create Account**.

٢. أمّا أنتم فتحتاجون إلى حساب المستخدم المسؤول **Computer Administrator**. انتبهوا لا يمكن أن تطبقوا الرّقابة الأبويّة على حساب المستخدم المسؤول بل على الحساب المحدود.

٣. لتشغيل عناصر تحكّمكم على حساب أطفالكم، اتبعوا الخطوات الآتية:

شغّلوا المراقبة الأبويّة من طريق النّقر على زرّ إبدأ Start، ثمّ على لوحة التّحكّم **Control Panel**، وبعد ذلك اختاروا **Parental Control**، وانقروا على **Manage Other Accounts**، ثمّ على إعداد المراقبة الأبويّة **Set Up Parental Controls**. إذا تمّت مطالبتكم بكلمة مرور مسؤول **Administrator Password** اكتبوها وأعيدوا كتابتها للتّأكيد **Confirm** ثمّ اضغطوا على **Ok**، اختاروا الحساب الّذي خلقتموه سابقًا، اختاروا **Enforce Current Settings**، **On**.

بعد تشغيل المراقبة الأبويّة يمكنكم التّحكّم في المجالات الآتية:

- **الحدود الزّمنيّة Time Limits:**

يمكنكم وضع حدود زمنيّة لتحديد الوقت المسموح به للأطفال للدّخول إلى جهاز الكمبيوتر. فهذا الخيار يسمح بتحديد ساعات معيّنة في كلّ يوم من أيّام الأسبوع للولوج إلى الحاسوب.

- **الألعاب Games:**
يمكنكم التّحكّم في الوصول إلى الألعاب، واختيار مستوى تصنيف العمر، ونوع المحتوى الّذي ترغبون في حظره، وتقرّرون ما إذا كنتم تسمحون بألعاب غير مصنّفة أو تمنعونها.
- السّماح باستخدام برامج محدّدة أو صدّها **Allow and block specific programs :**
يمكّنكم هذا الخيار من السّماح للأطفال باستخدام برامج معيّنة قمتم بتحديدها مسبقًا.

كيفية تقييد المواقع الّتي يمكن للأطفال زيارتها:
يمكنكم السّماح للأطفال بزيارة مواقع معيّنة أو عدم السّماح بذلك، وبيان ما إذا كنتم ترغبون في السّماح بتحميل الملفّات، ويمكنكم أيضًا تحديد المحتوى الّذي يمكن للأطفال تصفّحه على شبكة الإنترنت:

اذهبوا إلى **Start** ومنها إلى **Control Panel** ثمّ اختاروا **Internet Options** ، من بعدها اختاروا حقل **Contents** ، وعند الجزء الخاصّ ب **Content advisor** اضغطوا على **Enable** ، فتظهر شاشة تطلب إليكم إدخال كلمة سرّ**Password** فتدخلونها وتضغطون على **ok** ، ثمّ **اضغطوا** على **ok** الموجودة في شاشة تأكيد تمكين التّحكّم، من بعدها على كلمة **Setting** فتظهر قائمة اختاروا منها **Approved sites** حيث يمكنكم إضافة عنوان الموقع غير المرغوب به، والضّغط على **Never** ، أو إضافة عنوان الموقع المرغوب به والضّغط على **Always**.

كيفية تتبّع أنشطة الأطفال على الشّبكة:
هناك طرق عدّة لمعرفة المواقع الّتي يزورها الأطفال، مثل الدّخول إلىHistory الّذي سيعرض المواقع الّتي تمّت زيارتها في أيّام وأوقات محدّدة.
للدّخول إلىHistory اتبعوا الخطوات الآتية:
اذهبوا إلى **Start** ومنها إلى **control panel**، ثمّ اختاروا **internet options** ، من بعدها اختاروا حقل **General**، ثمّ **Browsing History** وبعدها **settings**، وفي **history** حدّدوا عدد الأيّام الّتي يجب أن يقوم متصفّح الإنترنت بالاحتفاظ بلائحة المواقع الّتي تمّت زيارتها. قوموا بهذه الخطوة مرة واحدة. وفي كلّ مرة تريدون الاطلاع على المواقع الّتي تمّت زيارتها. افتحوا متصفّح الإنترنت **internet explorer** مثلًا واختاروا **view** ثمّ **explorer bars** وبعدها **history** عندئذ ستظهر لكم إلى اليسار قائمة بالمواقع الّتي تمّت زيارتها مرتّبة وفاقًا لتواريخ تصفّحها.
وأخيرًا يتعيّن أن تكون رسائل السّلامة على الإنترنت حسنة التّوقيت، وحسّاسة ثقافيّا، وتُضاهي قِيَم المجتمع الّذي يعيش فيه الطّفل وقوانينه.
فالمبدأ الرّاسخ يقضي بترشيد استخدام الإنترنت عند الأطفال، ويكمن ذلك في احترام حقّهم في الوصول إلى التّكنولوجيا والإنترنت، وحضّهم على استغلال الشّبكة بطرق إيجابيّة ومفيدة، وممارسة مواطنيتهم الرّقميّة بكلّ مسوؤليّة بعيدًا عن الرّقابة البوليسيّة والمقاربة السّلبية.

كيفية الاستفسار والإبلاغ عن الشكاوى.
خط الشكاوى التابع لمكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي: ٠١/٢٩٣٢٩٣
للاستفسار عن أيّ مشكلة.
زيارة الموقع الإلكتروني **www.himaya.org** والاستفادة من خدمة e-helpline الّتي يوفّرها الموقع المذكور.

لائحة بمواقع آمنة ومفيدة للأطفال:

باللّغة الإنكليزيّة:

www.kidgrid.com
www.zilladog.com
www.kidsites.com
www.kidsites.org
www.scienceschool.com
www.mathsnet.net
www.funbrain.com
www.kidsnetsoft.com
www.kidsolr.com
www.go4english.com
www .kidsclick .org
yahooligans .yahoo .com
www .ajkids .com
www.ixl.com

باللّغة العربيّة:

http://www.kids.jo/main
http://net.hanaa.net/kidssites.htm
http://www.mbc3.net
http://zamzamworld.com
http://www.spacetoon.tv
http://www.atfalmasr.com
http://www.rafed.net/child/stories

باللّغة الفرنسيّة:

www.lesitepourenfants.com
www.sitespourenfants.com
www.petalia.org/fr_others.html
www.gofrette.com
www.fiaf.org/kids/links.html

مواقع تبقي الأهل على اطلاع دائم حول سلامة أطفالهم على الإنترنت:

www.kidsnetsoft.com/html/safety.html
www.internetsanscrainte.fr

محرّكات بحث للأطفال Search Engine For Kids :

http:// quinturakids.com
http://www.kidrex.org
http://www.askkids.com
http://kids.yahoo.com
http://www.squirrelnet.com/search/Google_SafeSearch.asp
http://www.googleforkid.com

من أجل الإبلاغ عن الشكاوى.

خط الشكاوى التابع لمكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي: ٠١/٢٩٣٢٩٣

للاستفسار عن أيّ مشكلة.

زيارة الموقع الإلكتروني **www.himaya.org** والاستفادة من خدمة e-helpline الّتي يوفّرها الموقع المذكور.

بعض المصادر:

- ويكيبيديا
- childdevelopmentinfo.com
- مطويّتا "سلامة أطفالنا على الشّبكة" و "تمتّع على الإنترنت بتجربة آمنة" اللّتان تمّ إنتاجهما بالتّعاون مع وزارة الشّؤون الاجتماعيّة والمركز التّربوي للبحوث والإنماء، وبعض الجمعيّات المحلّيّة.

إسمي الكامل
عنوان منزلي
عنوان مدرستي
هاتف منزلي

ما تنشر* حالك Online

* كلّ ما يُنشر على الإنترنت يُصبح بمتناول الجميع ولا يُمكن استرداده، فمن السّهل استغلاله للإساءة إليّ أو لتشويهه من قبل الآخرين، لذلك:

- أنا أتجنّب نشر أيّة معلومات شخصيّة تخصّني أو تخصّ عائلتي (اسمي الكامل، عنوان منزلي، صور، عنوان مدرستي،...).
- أنا لن أُجيب عن أيّة رسالة إلكترونية يُطلب فيها مني إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة مهما كانت مغرية.
- أنا أختار اسم مستخدم وكلمة مرور حيث لا يكشفان عن أيّة معلومات شخصية تخصّني.
- أنا أستفيد من أدوات الخصوصيّة (Privacy Settings) للحفاظ على معلوماتي التي لا أريد أن أتشاركها مع الجميع.



المعلومات الشّخصيّة والتواصل الآمن

١- أنا ومعلوماتي الشّخصيّة

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:
- يعرف أنواع المعلومات الشّخصيّة.
- يتعرّف إلى بعض مخاطر نشر معلومات شخصيّة على الشّبكة.
- يتعرّف إلى بعض القواعد الأساسيّة لحماية المعلومات الشّخصيّة.

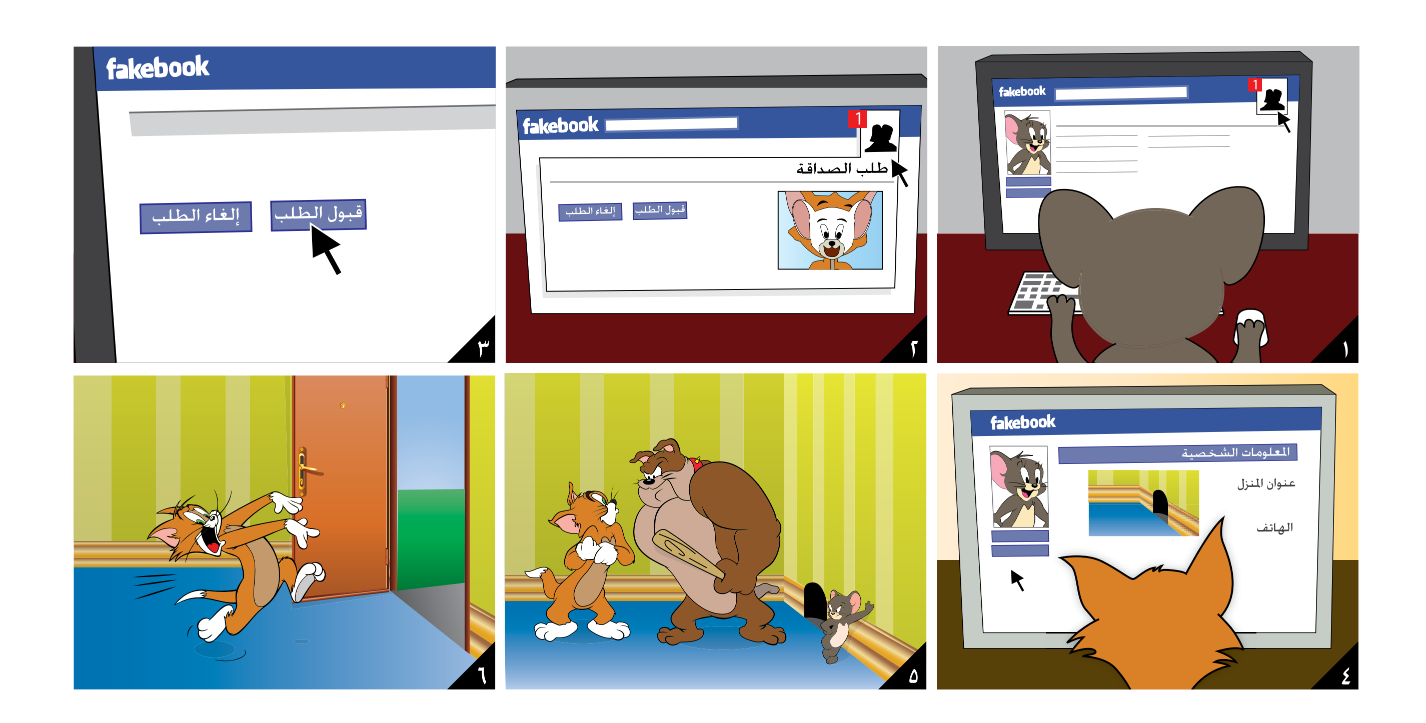
المعارف	المهارات والقدرات	المواقف
• ماهيّة المعلومات الشّخصيّة. • حدود استخدام الشّبكة.	• يحدّد المعلومات الشّخصيّة. • يميّز المعلومات الشّخصيّة من المعلومات العامّة. • يعدّد بعض مخاطر نشر معلومات شخصيّة على الشّبكة. • يميّز ما هو مسموح على الشّبكة ممّا هو غير مسموح. • يكتب كلمة مرور محصّنة، واسم مستخدم بمساعدة شخص راشد.	• يلتزم بعدم نشر معلومات شخصيّة على الشّبكة. • يرفض تبادل أيّة معلومات شخصيّة مع الغريب على الإنترنت. • يستشير شخصًا راشدًا يثق به (ليخبره عن أيّ شيء أو شخص يزعجه على الإنترنت، وقبل نشر أيّة صور أو فيديوهات أو الحالةstatus ، وقبل استعمال المعلومات من أيّ موقع، من أجل التّأكّد من محتوى اتفاقيات البرامج والتّطبيقات (applications) قبل الموافقة عليها، والتّحقّق من بيانات أي طلب ضمّ إلى قائمة الأصدقاء قبل الموافقة عليه).

- **الفئة المعنيّة:** تلامذة الصّفّين الرّابع والخامس من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٨...١٥، لوحة «ما تنشر حالك online»، شريط مصوّر الهرّ والفأر، شريط مصوّر الهرّ والعصفورة تاتي، فيديو «المواطنيّة الرّقميّة»، مطويّة الأطفال.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (١٥ دقيقة):

- يقسّم المعلّم/ة الصّفّ إلى أربع مجموعات، ويعطي كلّ مجموعة الشّريط المصوّر الآتي (مستند ١)، ويطلب إلى كلّ مجموعة التّدّقيق بالمضمون.



- تختار كلّ مجموعة مقرّرًا لها لسرد ما حصل مع الفأر.

- يسأل المعلّم/ة أسئلة عدّة وصولًا إلى تحديد ماهيّة المعلومات الشّخصيّة وأنواعها:
  - كيف عرف الهرّ مكان الفأر؟ (عنوان المنزل).
  - ماذا كان ليحصل لو لم يكن الكلب موجودًا؟ (إجابة حرّة).
  - ما نوع هذه المعلومة: علميّة، أم شخصيّة، أم ثقافيّة؟ (شخصيّة).
  - من يحدّد معلومات أخرى شبيهة بها؟ (الصّفحات الخارجيّة للشّخص، معلومات متعلّقة بأفراد عائلته، أرقام وعناوين خاصّة).
  - ما الفرق إذا بين المعلومات العامّة والمعلومات الشّخصيّة؟ (العامّة: مشتركة مع الجميع، أمّا الشّخصيّة فهي متعلّقة بالشّخص نفسه).

مرحلة التّعلّم: (٢٥ دقيقة)

- يقسّم المعلّم/ة الصّفّ إلى أربع مجموعات، ويعطي كلّ مجموعة الشّريط المصوّر الآتي (مستند ٢)، ويطلب إلى كلّ مجموعة التدّقيق بالمضمون.



- يسأل المعلّم/ة التّلامذة أسئلة عدّة وصولاً إلى تحديد مخاطر نشر معلومات شخصيّة على الشّبكة، وكيفيّة حمايتها:
  – ما الّذي مكّن الهرّ من الوصول إلى تاتي؟ (ما نشرته تاتي على صفحتها).

- يوزّع المعلّم/ة الجدول الآتي (وثيقة العمل ١)، ويطلب إليهم العمل ضمن مجموعات وملء العمود الأوّل فقط.

ما ننشره على الصّفحة			
الاسم الكامل			
نتيجة سباق الخيول...			

- يجمع المعلّم/ة الجداول ويعيد توزيعها بشكل عشوائي على المجموعات، ويطلب إلى كلّ مجموعة كتابة عنوان العمود الثّاني (ما يسمح بنشره) والثّالث (غير مسموح نشره)، والرّابع (السّبب).
- تقرأ كلّ مجموعة ما وصلها، وتضع أمام كلّ جملة إشارة تتوافق مع عنوان العمود.

ما ننشره على الصّفحة	صحيح أن ينشر	غير صحيح أن ينشر	السّبب
الاسم الكامل		–	معلومات شخصيّة
نتيجة سباق الخيول...	–		معلومات عامّة
اسم النّادي الّذي أرتاده		–	معلومات شخصيّة

- يكرّر المعلّم/ة العمليّة نفسها أيّ أنّه يجمع الجداول، ويعيد توزيعها بشكل عشوائي على المجموعات، ويطلب الى كلّ مجموعة كتابة عنوان العمود الخامس (مخاطر النشر).
- تقرأ كلّ مجموعة ما وصلها ،وتذكر مخاطر النّشر.

ما ننشره على الصّفحة	صحيح أن ينشر	غير صحيح أن ينشر	السّبب	مخاطر النّشر
الاسم الكامل		–	معلومات شخصيّة	تتبّعك من قبل شخص ما
نتيجة سباق الخيول...	–		معلومات عامّة	
اسم النّادي الّذي أرتاده		–	معلومات شخصيّة	التّحرّش

- وينهي المعلّم/ة النّشاط بالسّؤال الآتي: «كيف تتصرّفون لحماية معلوماتكم الشّخصيّة على الشّبكة؟»
- يفكّر كلّ تلميذ بحلّ بشكل فردي، يتلقّى المعلّم/ة الإجابات، ويكتبها على اللّوح بعد مناقشتها جماعيًّا وصولا إلى تحديد القواعد الأساسيّة لحماية المعلومات الشّخصيّة، فتكتبها كلّ مجموعة في الخانة الأخيرة من الجدول، وتحتفظ بها.

ما ننشره على الصّفحة	صحيح أن ينشر	غير صحيح أن ينشر	السّبب	مخاطر النّشر
الاسم الكامل		–	معلومات شخصيّة	تتبّع شخص لك
نتيجة سباق الخيول...	–		معلومات عامّة	
اسم النّادي الّذي أرتاده		–	معلومات شخصيّة	التّحرّش
قواعد حماية المعلومات الشّخصيّة:				

ما ننشره على الصّفحة	صحيح أن ينشر	غير صحيح أن ينشر	السّبب	مخاطر النّشر
الاسم الكامل		–	معلومات شخصيّة	تتبّعك من قبل شخص ما
نتيجة سباق الخيول...	–		معلومات عامّة	
اسم النّادي الّذي أرتاده		–	معلومات شخصيّة	التّحرّش
	الأمثلة كثيرة ووافرة لكن تمّ ذكر البعض منها على سبيل المثال لا الحصر....			

قواعد حماية المعلومات الشّخصيّة:

- ألتزم بعدم نشر معلومات شخصيّة على الشّبكة.
- أرفض تبادل أيّة معلومات شخصيّة مع الغريب على الإنترنت.
- أستشير شخصًا راشدًا، أثق به، قبل نشر أيّة صور أو فيديوهات أو الحالةstatus .
- أستشير شخصًا راشدًا، أثق به، قبل قراءة أيّة معلومات من أيّ موقع، أو استعمالها أو تحميلها.
- أستشير شخصًا راشدًا، أثق به، للتّأكّد من محتوى اتفاقيات البرامج والتّطبيقات (applications) قبل الموافقة عليها.
- أستشير شخصًا راشدًا، أثق به، للتّأكّد من بيانات أي طلب ضمّ إلى قائمة الأصدقاء قبل الموافقة عليه.
- أكتب كلمة مرور محصّنة، واسم مستخدم بمساعدة شخص راشد.

التّطبيق: (١٠ دقائق)

• يوزّع المعلّم/ة وثيقة العمل ١، ويعمل التّلامذة على حلّها، بشكل إفرادي، وتتمّ المناقشة جماعيًّا.

١- أضع إشارة في المكان المناسب في الجدول:

المعلومة	معلومات شخصيّة	معلومات عامّة
تكون الحرارة مرتفعة ظهرًا.		-
الاسم.	-	
مكان عمل الوالد.	-	
موقع قلعة بعلبك.		-
البريد الإلكتروني.	-	
رقم هاتفي.	-	
شكل الكرة الأرضيّة.		-

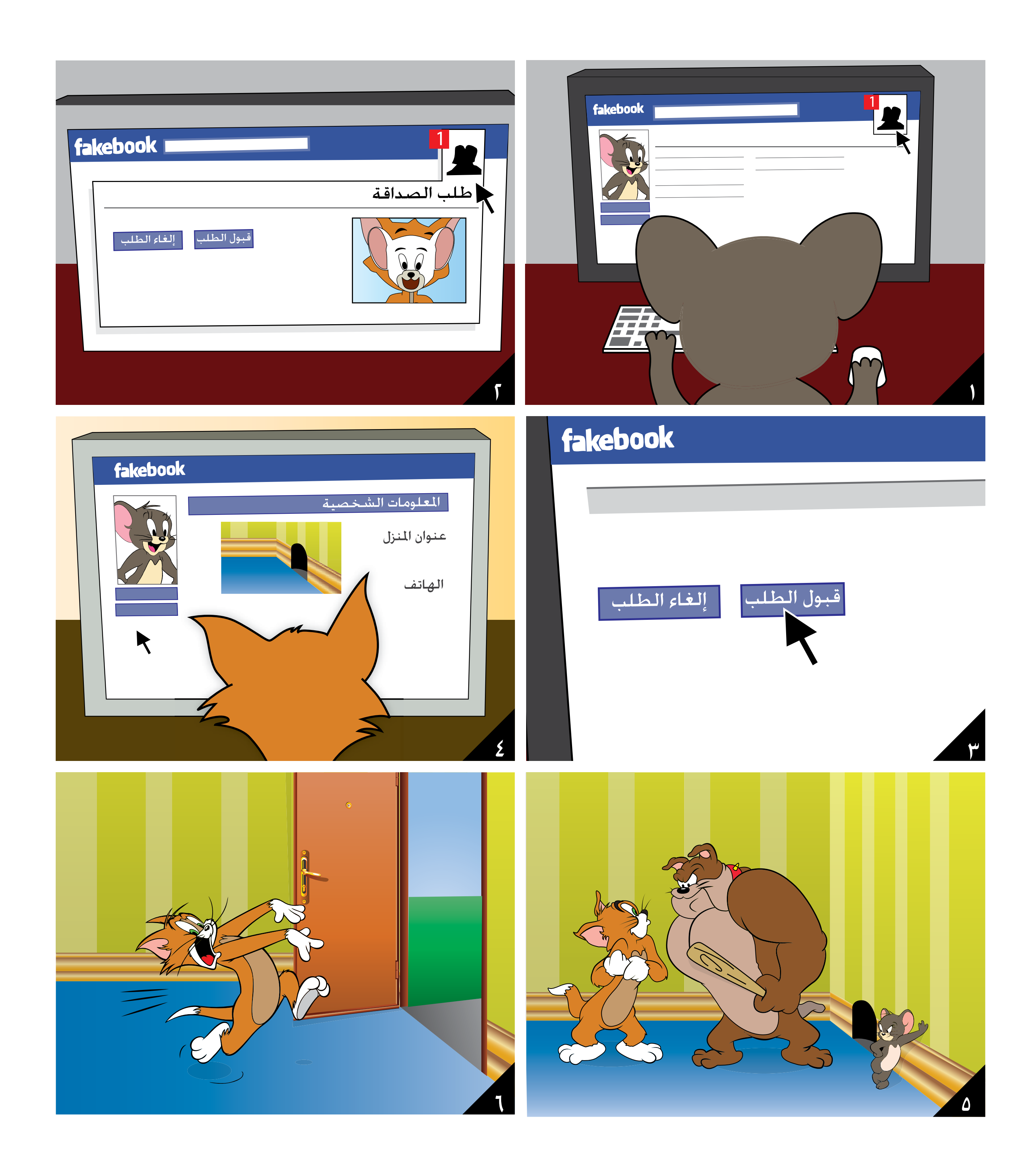
٢- أحوّق المعلومات الّتي لا يتوجّب عليّ عرضها على صفحات مواقع التّواصل الاجتماعي، موضّحًا اختياري:
طولي- عنوان مدرستي- اسم كتاب القراءة- لون البحر- لون شعري- رمز الدّخول السّريّ.
يحوّق التّلامذة: (الطول، عنوان المدرسة، لون الشّعر، رمز الدّخول السّريّ لأنها معلومات شخصيّة).

٣- أصف شعوري عند رؤيتي لصور عائلتي معلّقة في المدرسة.... (الشّعور يكون إمّا سلبيًا وإمّا إيجابيًا).

٤- أذكر طريقة كتابة كلمة السّرّ هذه (pa@!ss2#wo3$rd4%)، وأكتب كلمة سرّ على غرارها. (الإجابة: تحوي أحرفًا وأرقامًا ورموزًا).

ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

مستند ١


fakebook
1
١
fakebook
1
طلب الصداقة
قبول الطلب
إلغاء الطلب
٢
fakebook
قبول الطلب
إلغاء الطلب
٣
fakebook
المعلومات الشخصية
عنوان المنزل
الهاتف
٤
٥
٦

مستند ٢


١
fakebook
تاتي
تاتي ذاهبة إلى البحر المجاور لبيتها
٢
تاتي ذاهبة إلى البحر المجاور لبيتها
٣
٤

وثيقة العمل ١

ما ننشره على الصّفحة				

وثيقة العمل ٢

١- أضع إشارة في المكان المناسب في الجدول:

المعلومة	معلومات شخصيّة	معلومات عامّة
تكون الحرارة مرتفعة ظهرًا		
الاسم		
مكان عمل الوالد		
موقع قلعة بعلبك		
البريد الالكتروني		
رقم هاتفي		
شكل الكرة الأرضيّة		

٢- أحوّق المعلومات الّتي لا يتوجّب عليّ عرضها على صفحات مواقع التّواصل الاجتماعي، موضّحًا اختياري:

طولي- عنوان مدرستي- اسم كتاب القراءة- لون البحر- لون شعري- رمز الدّخول السّريّ.

٣- أصف شعوري عند رؤيتي لصور عائلتي معلّقة في المدرسة....

٤- أذكر طريقة كتابة كلمة السّرّ هذه (pa@!ss2#wo3$rd4%)، وأكتب كلمة سرّ على غرارها.

٢- أحمي معلوماتي الشّخصيّة

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:
- يعرف أنواع المعلومات الشّخصيّة.
- يتعرّف إلى بعض مخاطر نشر معلومات شخصيّة على الشّبكة.
- يتعرّف إلى بعض القواعد الأساسيّة لحماية المعلومات الشّخصيّة.

المعارف	المهارات والقدرات	المواقف
• ماهيّة المعلومات الشّخصيّة. • ماهيّة مبدأ الحرمة الشّخصيّة على الإنترنت. • حدود استخدام الشّبكة.	• يحدّد المعلومات الشّخصيّة. • يميّز المعلومات الشّخصيّة من المعلومات العامّة. • يعدّد مخاطر نشر معلومات شخصيّة على الشّبكة. • يميّز ما هو مسموح على الشّبكة ممّا هو غير مسموح. • يفرّق بين الصّور والفيديوهات والحالة الشّخصيّة الآمنة status • يكتب كلمة مرور محصّنة، واسم مستخدم معيّن.	• يلتزم بعدم نشر معلومات شخصيّة على الشّبكة. • يرفض تبادل أيّة معلومات شخصيّة مع الغريب على الإنترنت. • يستشير شخصًا راشدًا يثق به (ليخبره عن أيّ شيء أو شخص يزعجه على الإنترنت، وللاستفادة من أدوات الخصوصيّة، وقبل استعمال المعلومات من أيّ موقع، من أجل التّأكّد من محتوى اتفاقيات البرامج والتّطبيقات (applicationss) قبل الموافقة عليها ، والتّحقّق من بيانات أيّ طلب ضمّ إلى قائمة الأصدقاء قبل الموافقة عليه).

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٨...١٥، لوحة «ما تنشر حالك online»، فيديو فكّر قبل ما تنشر، شريط مصوّر «صورة القرد»، فيديو «المواطنيّة الرّقميّة»، مطويّة الأطفال.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (٥ دقائق):

- يطلب المعلّم/ة إلى كلّ تلميذ التّنقّل في الصّفّ واختيار شخص ما والعمل معه على ملء الإستمارة الآتية:

الاسم الكامل	**اسم الوالد**	**مكان السّكن**	**رقم الهاتف**
عدد الأخوة والأخوات	**الطّول**	**لون العينين**	**عنوان المنزل**
البريد الإلكتروني	**الكتاب المفضّل**	**البرنامج المفضّل**	**اسم المدرسة**
موقع قلعة صور	**اسم جبل في لبنان**	**سعر لوح الشّوكولا**	**ألوان قوس قزح**
موقع قلعة بعلبك	**تاريخ الولادة**	**رقم هاتفي**	**شكل الكرة الأرضيّة**

- يسأل التّلامذة: «ماذا لاحظتم أثناء ملء الإستمارة؟» ما هي المعلومات الشّخصيّة الواردة في الجدول، وما هي المعلومات العامّة؟

- ماذا تستنتجون؟ (الإجابة: لكلّ شخص بيانات شخصيّة مختلفة عن الآخر...).

مرحلة التّعلّم: (٣٠ دقيقة)

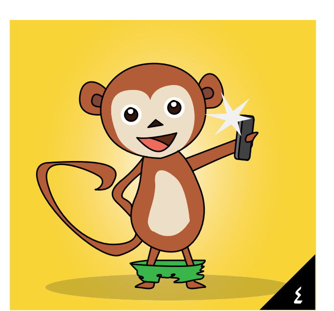
- يشاهد التّلامذة فيديو «فكّر قبل ما تنشر»، ويصار إلى مناقشة المضمون وصولًا إلى خلاصة مفادها ضرورة التّفكير قبل نشر أيّ شيء خاص على الشّبكة.

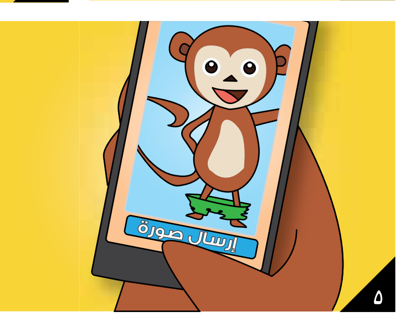
- وفي حال عدم توافر آلة عرض، يوزّع المعلّم/ة على التّلامذة الشّريط المصوّر «صورة القرد، مستند ١».
- تتمّ المناقشة وصولًا إلى خلاصة مفادها ضرورة التّفكير قبل نشر أيّ شيء خاص على الشّبكة. وضرورة المحافظة على معلوماتنا الشّخصيّة.















- يكتب المعلّم/ة على اللّوح الجملة الآتية: « مشاكل ناتجة من نشر معلومات شخصيّة على الإنترنت»، ويطلب إلى التّلامذة الصّعود إلى اللّوح كلّ بدوره وكتابة كلمة أو جملة تدور حولها ليصار إلى تجميع المخاطر النّاجمة عن هذا الفعل.

- يقسّم المعلّم/ة الصّفّ إلى خمس مجموعات، يعطي كلّ مجموعة جملتين من الجمل الواردة في الجدول أدناه (وثيقة عمل ٢)، ويطلب إلى كلّ مجموعة إبداء رأيها حول ما هو وارد فيها ليصار بعد ذلك إلى مناقشتها جماعيًّا:

أغيّر معلوماتي الشّخصية على موقع الفايس بوك عندما أدردش مع شخص غريب.	لا خطر من ذكر اسمي الكامل لشخص ما على الإنترنت لأنّه لا يعرفني.
لا أحد يستطيع سرقة الرّمز السّرّي.	أفتح حسابًا على إحدى شبكات التّواصل الاجتماعي مستخدما اسم شخصيّة معروفة.
لا يهمّني مصدر المعلومات الّتي أحمّلها عن الإنترنت.	أوافق على التّطبيقات جميعها من دون مراجعتها.
أنشر صوري جميعها ليتعرّف إليّ أكبر عدد من الأشخاص.	أستشير شخصًا راشدًا أثق به ليساعدني على الاستفادة من أدوات الخصوصيّة.
أقبل كلّ من يرسل إليّ طلبات صداقة.	أنشر أيّ فيديو وفاقًا لعنوانه من دون أن أشاهده.

• **بعض الإجابات:**
- أغيّر معلوماتي الشّخصية على موقع الفايس بوك عندما أدردش مع شخص غريب. (خطأ، يجب رفض تبادل معلومات شخصيّة مع الغريب).
- لا أحد يستطيع سرقة الرّمز السّرّي. (خطأ، يمكن لأيّ كان سرقة الرّمز السّرّي إذا لم يكتب بشكل قويّ أي يحوي حروفًا ورموزًا وأرقامًا).
- لا يهمّني مصدر المعلومات الّتي أحمّلها عن الإنترنت. (خطأ، معظم المعلومات على الإنترنت غير موثوق بها، لأنّه تعبّر أحيانا عن وجهة نظر أصحابها، ولا تمتّ إلى الحقيقة بأيّة صلة).
- أنشر صوري جميعها ليتعرّف إليّ أكبر عدد من الأشخاص. (خطأ، لأنّ الصّور هي معلومات شخصيّة، ونشرها يسبّب لي مشاكل، وممكن أن يستغلّها أحد بشكل يسيء إليّ).
- لا أقبل كلّ من يرسل إليّ طلبات صداقة. (صح)
- لا خطر من ذكر اسمي الكامل لشخص ما على الإنترنت لأنّه لا يعرفني. (خطأ، لأنّه من خلال اسمك الكامل يمكنه الاستدلال على عنوانك والإساءة إليك، أو إلى أهلك).
- أفتح حسابًا على إحدى شبكات التّواصل الاجتماعي مستخدمًا اسم شخصيّة معروفة. (خطأ، لأنّ ذلك قد يعرّضك للملاحقة القانونيّة، ويوقعك بمشاكل عديدة).
- أوافق على التّطبيقات جميعها من دون مراجعتها. (خطأ، يمكن الموافقة عليها بعد مراجعتها مع شخص راشد).
- أستشير شخصًا راشدًا أثق به ليساعدني على الاستفادة من أدوات الخصوصيّة. (صح)
- أنشر أيّ فيديو وفاقًا لعنوانه من دون أن أشاهده. (خطأ، لأنّ المضمون يمكن أن يحوي رسائل مسيئة لمعتقداتك، ولبيئتك).
- يطلب المعلّم/ة إلى التّلامذة، وبناء على ما تمّت مناقشته في الخطوة الثّانية، وبالاستناد إلى مكتسباتهم السّابقة، أن يذكروا بعض القواعد الأساسيّة لحماية المعلومات الشّخصيّة، ويصنعوا منها وثيقة يوقّع الجميع عليها.

التّطبيق: (١٠ دقائق)

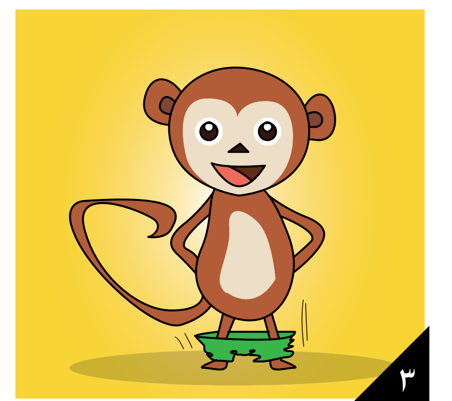
- يعمل التّلامذة إفراديًا على حلّ الأسئلة الواردة في الوثيقة ٣، وتتمّ المناقشة جماعيًّا.
- الإجابة عن السّؤال ١: كلّ ما ننشره على الشّبكة يبقى ولا يمحى، ولا نعرف إلى يد أيّ شخص سيصل، ولا حتّى كيفيّة استخدامه له. وبما أنّ المعلومات الشّخصيّة لكلّ منّا تشكّل حاليًّا الكنز الأغلى ثمنًا عاليًّا علينا المحافظة عليها بأيّ ثمن كان، وبكلّ وعي.
- توضيح عن السّؤال ٣: الرّمز السّرّي مؤلّف من رموز وحروف وأرقام وهو عبارة عن اختصار لكلمات جملة مفيدة. على سبيل المثال لا الحصر: J'ai une cassette et huit cd = G1K7&8CD

ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

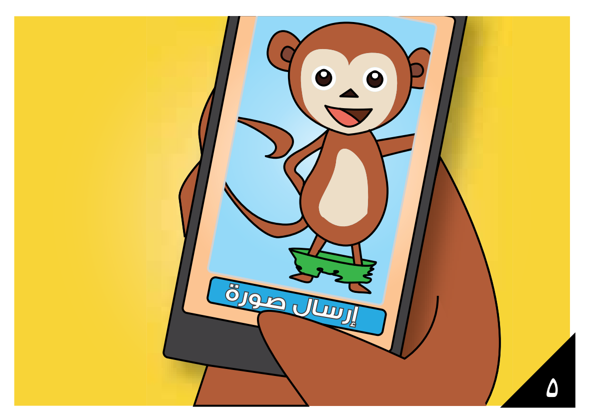
مستند ١















وثيقة عمل ١

الاسم الكامل	اسم الوالد	مكان السّكن	رقم الهاتف
عدد الأخوة والأخوات	الطّول	لون العينين	عنوان المنزل
البريد الإلكتروني	الكتاب المفضّل	البرنامج المفضّل	اسم المدرسة
موقع قلعة صور	اسم جبل في لبنان	سعر لوح الشّوكولا	ألوان قوس قزح
موقع قلعة بعلبك	تاريخ الولادة	رقم هاتفي	شكل الكرة الأرضيّة

وثيقة عمل ٢

أغيّر معلوماتي الشّخصيّة على موقع الفايس بوك عندما أدردش مع شخص غريب.
لا أحد يستطيع سرقة الرّمز السّرّي.
لا يهمّني مصدر المعلومات الّتي أحمّلها عن الإنترنت.
أنشر صوري جميعها ليتعرّف إليّ أكبر عدد من الأشخاص.
أقبل كلّ من يرسل إليّ طلبات صداقة.
لا خطر من ذكر اسمي الحقيقي لشخص ما على الإنترنيت لأنّه لا يعرفني.
أفتح حسابًا على إحدى شبكات التّواصل الاجتماعي مستخدمًا اسم شخصيّة معروفة.
أوافق على التّطبيقات جميعها من دون مراجعتها.
أستشير شخصًا راشدًا أثق به ليساعدني على الاستفادة من أدوات الخصوصيّة.
أنشر أيّ فيديو وفاقًا لعنوانه من دون أن أشاهده.

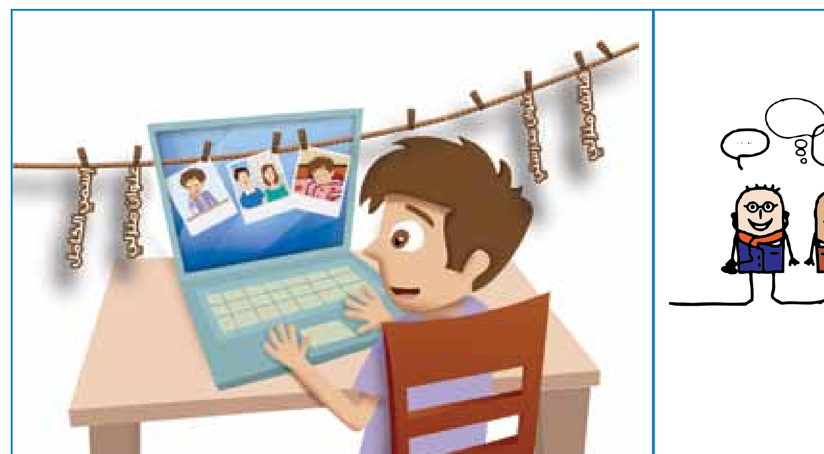
وثيقة عمل ٣

١- أكتب تعليقًا تحت كلّ صورة.

٢- أجد صلة وصل بين هذه الصّور.

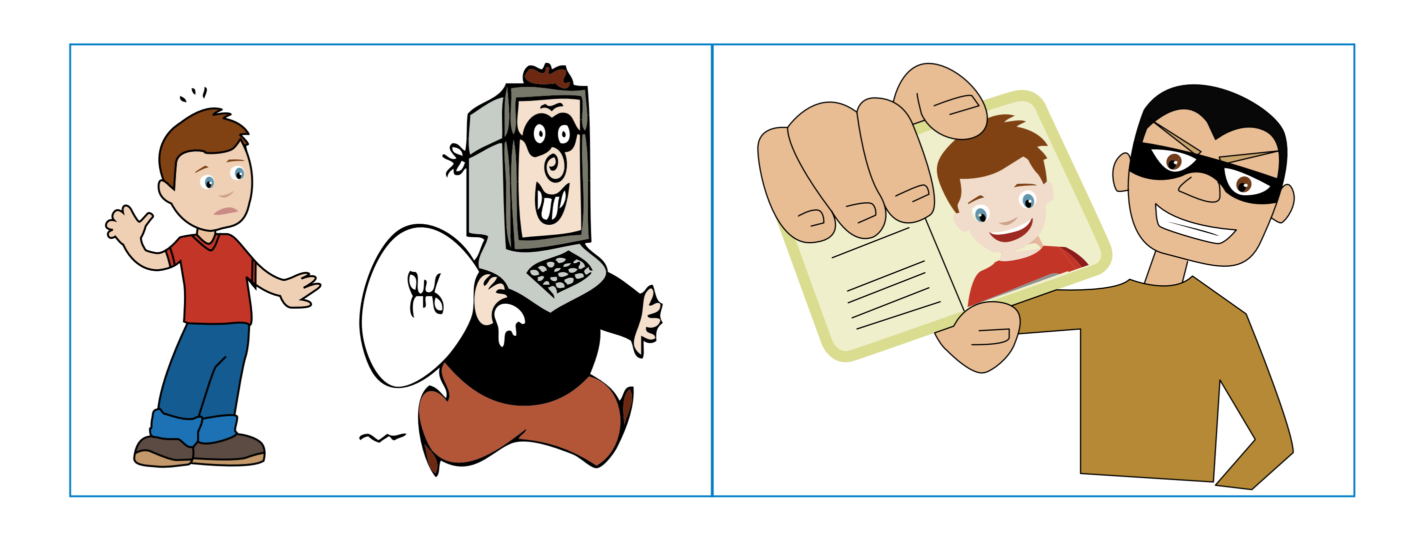
....





....

....



....

....

٣- ألاحظ الرّمز السّري الآتي:G1K7&8CD، وأذكر طريقة كتابته، ثمّ أحاول أن أكتب رمزًا خاصًّا بي على غراره.

....

٣- أنا دقيق في ما يخصّني

الكفاية الأولى: في نِهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:
- يعرف أنواع المعلومات الشّخصيّة.
- يتعرّف إلى مخاطر نشر معلومات شخصيّة على الشّبكة.
- يتعرّف إلى بعض القواعد الأساسيّة لحماية المعلومات الشّخصيّة.

المعارف	المهارات والقدرات	المواقف
• ماهيّة المعلومات الشّخصيّة. • ماهية مبدأ الحرمة الشّخصيّة على الإنترنت. • حدود استخدام الشّبكة.	• يحدّد المعلومات الشّخصيّة. • يميّز المعلومات الشّخصيّة من المعلومات العامّة. • يعدّد مخاطر نشر معلومات شخصيّة على الشّبكة. • يميّز ما هو مسموح على الشّبكة ممّا هو غير مسموح. • يفرّق بين الصّور والفيديوهات والحالة الشّخصيّة الآمنة status. • يكتب كلمة مرور محصّنة، واسم مستخدم معيّن.	• يلتزم بعدم نشر معلومات شخصيّة على الشّبكة. • يرفض تبادل أيّة معلومات شخصيّة مع الغريب على الإنترنت. • يستفيد من أدوات الخصوصيّة. • يتأكّد من المواقع قبل قراءة أيّة معلومات أو استعمالها أو تحميلها. • يراجع محتوى اتفاقيات البرامج والتّطبيقات (applications) قبل الموافقة عليها.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٨...١٥، لوحة «ما تنشر حالك online»، فيديو ما تنشر حالك، فيديو المواطنيّة الرّقميّة، شريط مصوّر الحرامي والرّجل، مطويّة الأطفال.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (٥ دقائق)

- يقسّم المعلّم/ة الصّفّ إلى مجموعات عمل، يوزّع لكلّ منها الصّورة التّالية، ويطلب إلى كلّ منها التّعليق على مضمونها ليصار إلى المناقشة بعد طرح السّؤال الآتي: لو كنت مكانه كيف تتصرّف؟



مرحلة التّعلّم: (٣٥ دقيقة)

- يقسّم المعلّم/ة الصّفّ إلى أربع مجموعات عمل، ويوزّع على كلّ مجموعتين صورة:

المجموعتان ١–٢ (الوثيقة ١):



المجموعتان ٣–٤ (الوثيقة ٢):



- يطلب المعلّم/ة إلى كلّ مجموعة تخيّل القصّة الّتي جرت في الصّورتين أعلاه ليصار إلى مناقشتها جماعيًّا .
- بعد ذلك تملأ كلّ مجموعة الجدول الآتي بما يناسب:

مشاكل ناتجة من نشر معلومات شخصيّة على الشّبكة	القواعد الأساسيّة لحماية المعلومات الشّخصيّة
سرقة معلوماتي الشّخصيّة، التّحرش، الإساءة إليّ أو إلى أهلي،	يلتزم بعدم نشر معلومات شخصيّة على الشّبكة.
	يرفض تبادل أيّة معلومات شخصيّة مع الغريب على الإنترنت.
	يستفيد من أدوات الخصوصيّة.
	يتأكّد من المواقع قبل قراءة أيّة معلومات أو استعمالها أو تحميلها.
	يراجع محتوى اتفاقيات البرامج والتّطبيقات (applications) قبل الموافقة عليها.
	يكتب كلمة مرور محصّنة، واسم مستخدم معيّن....

- بعد مرور ١٥ دقيقة، يجمع المعلّم/ة النّتاجات ويعيد توزيعها على مجموعات مختلفة ليصار إلى قراءة ما تحويه من معلومات وإضافة نقاط غير مذكورة، أو حذف نقاط غير ملائمة.
- يتمّ إنهاء هذا الجزء بمناقشة النّتاجات وتوحيدها.

التّطبيق: (١٥ دقيقة)

- يعمل التّلامذة إفراديًا على حلّ الأنشطة الواردة في الوثيقة ٣، وتتمّ المناقشة جماعيًا.

ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

وثيقة عمل ١



القصّة:

مشاكل ناتجة من نشر معلومات شخصيّة على الشّبكة	القواعد الأساسيّة لحماية المعلومات الشّخصيّة

وثيقة عمل ٢



القصّة:

مشاكل ناتجة من نشر معلومات شخصيّة على الشّبكة	القواعد الأساسيّة لحماية المعلومات الشّخصيّة

وثيقة عمل ٣

• أرسم داخل المربّع نموذجًا تفصيليًّا لصفحة مثاليّة على مواقع التّواصل الاجتماعي.

• أكتب رمزًا سرّيًّا قويًّا وأذكر كيفيّة كتابته.

• أبدي رأيي بفيديو «ما تنشر حالك».

الغريب* Online
ممكن يكون خطر Offline

*** هل أفتح باب المنزل للغريب؟ بالطبع لا، إذًا كما أتجنّب الغرباء في الواقع أتجنّبهم أيضًا على الإنترنت! لذلك:**

- أنا أرفض التّحدّث مع الغرباء على الإنترنت لأنّه من السهل انتحال شخصيّة غير حقيقيّة بعمر مزيّف وصورة مزيّفة بغرض الإساءة إليّ.

- أنا لا أُقابل شخصًا غريبًا تعرّفت إليه على الإنترنت إلاّ بموافقة أهلي ووجودهم.

- أنا لن أَنبهر بمديح الغرباء ووعودهم ولن أمتثل لإغراءاتهم كالمال، والهدايا، والحنان...

- أنا لن أُجيب عن الأسئلة المتعلقة بالبنية الجسدية (القامة، الوزن، لون العينين، السن...).

- أنا أُخبر دائمًا شخصًا راشدًا أثق به عن أيّ شيء أو أيّ شخص يُزعجني على الإنترنت لكي أحمي نفسي وأحمي غيري.



الغريب

١- صديق أم غريب؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظاً على سمعة رقميّة جيدة وحامياً جهازه ومعلوماته الشخصية من الخداع والاحتيال والبرمجيات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:

- يتعرّف إلى مفهوم الغريب.
- يعي بعض مخاطر التّواصل مع الغريب عبر الإنترنت.
- يتعرّف إلى بعض القواعد الأساسيّة للتّواصل الآمن مع الغريب عبر الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهيّة الغريب.	• يفرّق بين العلاقات الواقعيّة والافتراضيّة. • يفرّق بين الصّفحة الحقيقيّة والصّفحة الوهميّة Real & Fake Profile.	• يرفض التحدّث إلى الغرباء على الإنترنت أو مقابلتهم شخصيًّا. • يقطع أيّ محادثة أو دردشة لا توحي بالرّاحة.

- **الفئة المعنيّة:** تلامذة الصّفّين الرّابع والخامس من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص:٨-٩-١٠-٢٣-٢٦، اللّوحة الجداريّة «الغريب online ممكن يكون خطر offline»، ورقتي عمل «صديق مميّز» و «أتخيّل وأرسم»، فيديو الغريب ٢، فيديو المواطنيّة الرّقميّة.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة.

سير النّشاط:

التّحفيز (٧ دقائق):

- يخبر المعلّم/ة التّلامذة أنّ شخصين كانا يتحدّثان إلى بعضهما عبر الإنترنت، قال الأوّل للثّاني:

– عمري ١٢ سنة، شعري أشقر، وعيناي زرقاوتان، جميلة المظهر، فنّاني المفضّل هو جاستين بيبر، ألعب الجمباز، وأحبّ القطط البيضاء.

أخبر الثّاني الأوّل بما يأتي:
– اسمي راني، وأنا في الصّفّ السّادس، أنا كابتن فريق كرة القدم، وجاستين بيبر هو المغنّي المفضّل لدي أيضًا، لكنّي أفضّل الكلاب على القطط، وشعري بني، وأنا أسمر، وطويل القامة.

- يطلب المعلّم/ة إلى التّلامذة أن يرسموا الشّخصين الأوّل والثّاني ثمّ يشاهد رسوماتهم، ويخبرهم أنّه في نهاية الحصّة سوف يريهم صورة هذين الشّخصين.

- في حال توافرت أداة لعرض الفيديو يعرضه المعلّم/ة عليهم ويسألهم عمّا ينتظرونه من موضوع الحصّة.

مرحلة التّعلّم (٣٣ دقيقة):

- يطلب المعلّم/ة إلى التّلامذة أن يقرأوا مستند «صديق مميّز» بصمت، وينقسموا إلى مجموعات مؤلّفة من شخصين أو أربعة على الأكثر، ثمّ يتناقشوا مع بعضًا ليجيبوا عن الأسئلة المطروحة. وبعد أن ينتهوا، يناقش معهم النّقاط الآتية:

– هل بإمكان أيّ كان الإدعاء بأنّه شخص آخر على الإنترنت؟
– لمَ برأيكم يقوم بعض النّاس بإخفاء هويّتهم الحقيقيّة؟

- يعطي المعلّم/ة كلّ تلميذ/ة دائرة ورقيّة ملوّنة بالأخضر من جهة، وبالأحمر من جهة أخرى (يمكن وضع إشارة صح عوضًا عن الأخضر، وإشارة خطأ عوضًا عن الأحمر)، ويقرأ الجمل الآتية، ويطلب إليهم أن يرفعوا الجهة الحمراء في حال عدم تأييدهم الفكرة، والخضراء في حال أيّدوها مع تعليل مواقفهم:

  - **أضيف صديقًا إلى لائحة الأصدقاء إن كان من العمر نفسه ولدينا هوايات مشتركة.**
  (خطأ: إذ لا يمكننا أن نتأكّد من هويّة الشّخص على الإنترنت أو عمره أو نواياه).

  - **لا بأس إن تكلّمت مع غريب شرط أن أستخدم اسمًا مزيّفًا.**
  (خطأ: يمكن أن يكون منتحلا أيضًا شخصيّة مزيّفة، ونواياه سيّئة، كما يمكن أن يستدرجك ليتعرّف إلى هويّتك).

  - **لا بأس من إضافة صديق الصّديق إلى لائحة أصدقائي.**
  (خطأ: الشّخص الوحيد الّذي نضيفه إلى لائحة الأصدقاء هو الصّديق في الحياة الواقعيّة والّذي نعرفه وجهًا لوجه).

  - **إذا طلب منّي شخص لا أعرفه معلومات عنّي أو عن أصدقائي، أصدّه block على الفور.** (صح).

  - **لا بأس إذا قابلت الأشخاص الّذين تعرّفت إليهم على الإنترنت، ولكن في أماكن عامّة. مثل: المطاعم والأندية وإلى جانب المدرسة.**
  (خطأ لا نلتقي بالأشخاص الّذين نتعرّف إليهم عبر الإنترنت إلّا بموافقة الأهل وبحضورهم).

  - **لا بأس إذا قابلت الأشخاص اللّطفاء الّذين تعرّفت إليهم على الإنترنت.**
  (خطأ لا يمكننا أن نتأكّد من نوايا الأشخاص على الإنترنت لأنّه يمكن لأيّ شخص الإدعاء بصفات لا يمتلكها).

  - **أضيف صديقًا إلى لائحة الأصدقاء إذا أعجبني شكله.**
  (خطأ فبعض الأشخاص أصحاب النّوايا السّيّئة يزوّرون صورهم، فليس بالضّرورة أن يكون الشّخص الجميل، صافي النّيّة وذات أخلاق حميدة).

- **إذا كلّمني أحد بطريقة غير لائقة أصدّه، ولكنّني لن أخبر أحدًا لأنّني أستطيع أن أحمي نفسي.**
(خطأ: من الضّروري إبلاغ شخص راشد تثق به ليتصرّف).

- **قبل أن أضيف أيّ شخص إلى لائحة أصدقائي عليّ أن أتأكّد من أنّني أعرفه في حياتي الواقعيّة.** (صح).

- **أصدّ block كلّ غريب يطلب إليّ إضافته إلى لائحة الأصدقاء حتّى لو بدا لطيفًا جدًّا.** (صح).

- **لا بأس إذا زيّفت عمري واستخدمت غرف الدّردشة والشّبكات الاجتماعيّة الخاصّة بالكبار.**
(خطأ: هل تزيّف عمرك للحصول على رخصة قيادة؟ إذًا الأمر نفسه ينطبق على الإنترنت، وعليك الالتزام بالقواعد واحترامها لأنّها وجدت لحمايتك).

- **لا أجيب عن أيّة أسئلة متعلّقة بي مثل شكلي أو الأماكن الّتي أرتادها أو عنواني.** (صح).

- **لا بأس إذا أفصحت عن اسم النّادي أو دور السّينما المفضّلة لديّ لصديق تعرّفت إليه على الإنترنت.**
(خطأ: هذه معلومة شخصيّة تساعد أصحاب النّوايا السّيئة على تحديد مكانك. عليك أن لا تتبادل أيّة معلومات شخصيّة مع الغريب، لو كانت بسيطة).

- **كلّ من أضيفه إلى لائحة أصدقائي هو صديقي.**
(خطأ: الصّديق هو الشّخص الّذي تعرفه في حياتك الواقعيّة وتثق به، أمّا الأشخاص الّذين تعرفهم في حياتك الواقعيّة ولا تربطك بهم علاقة صداقة فنسمّيهم معارف).

- **إذا هدّدني أحد أو أزعجني في غرف الدّردشة أحلّ المشكلة بنفسي، ليس بالضّرورة أن أخبر أحدًا عنه.**
(خطأ: أصدّه block وأبلّغ شخصًا راشدًا أثق به، وأحفظ الرّسائل كدليل).

- **أستطيع أن أتاكّد من هويّة الشّخص الموجود على الإنترنت من خلال صوره ومعلوماته الشّخصيّة الموجودة على صفحته.**
(خطأ: لا يمكننا أن نتأكّد من نوايا الأشخاص على الإنترنت لأنّه يمكن لأيّ شخص الإدعاء بصفات لا يمتلكها).

التّطبيق (١٠ دقائق):

- يطلب المعلّم/ة إلى التّلامذة أن يعملوا بشكل فرديّ على وثيقة عمل «أتخيّل وأرسم».
وبعد الانتهاء، يريهم اللّوحة الجداريّة، ويخبرهم أنّ هذين الشّخصين هما اللّذان طلب إليهم أن يرسموهما في بداية الحصّة.



لو كنت مكان سامي، هل تضيف spiderman101 إلى لائحة أصدقائك؟ علّل إجابتك.

....

....

....

....

....

....

ما الّذي دفع بسامي لإضافة spiderman101 إلى لائحة أصدقائه؟

....

....

....

....

....

....

ما هي المعلومات الشّخصيّة الّتي طلبها spiderman101 من سامي؟

....

....

كيف يجب أن يتصرّف سامي؟

....

....

....

اختر النّهاية الّتي تؤدّي إلى مخاطر شارحًا السّبب:

أتخيّل وأرسم

أتخيّل ثمّ أرسم داخل المربّع:

لو كان الغريب على الإنترنت حيوانًا، لكان يشبه:

لو كان الغريب على الإنترنت شيئًا، لكان يشبه:

أرسم الشّخص البالغ الّذي أثق به وألجا إليه في حال حصلت معي أشياء مريبة على الإنترنت.

٢- من هو صديقي على الإنترنت؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على ان يتواصل بشكل آمن عبر الإنترنت، محافظاً على سمعة رقميّة جيدة وحامياً جهازه ومعلوماته الشخصية من الخداع والاحتيال والبرمجيات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:
- يتعرّف إلى مفهوم الغريب.
- يعي مخاطر التّواصل مع الغريب عبر الإنترنت.
- يتعرّف إلى القواعد الأساسيّة للتّواصل الآمن مع الغريب عبر الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهيّة الغريب. • طرق الحماية على الشبكة.	• يفرّق بين مفهوم الأصدقاء والمعارف. • يفرّق بين العلاقات الواقعيّة والافتراضيّة. • يفرّق بين الصّفحة الحقيقيّة والصّفحة الوهميّة Real & Fake Profile.	• يرفض التحدّث إلى الغرباء على الإنترنت أو مقابلتهم شخصيًّا. • يقطع أيّ محادثة أو دردشة لا توحي بالرّاحة.

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص:٨-٩-١٠-٢٣-٢٦، معلّقة «الغريب online ممكن يكون خطر offline»، مطويّة الأطفال والأهل، فيديو الغريب أو فيديو الغريب١، فيديو المواطنيّة الرّقميّة.
- **نمط التّنفيذ:** عمل مجموعات، نقاش.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق):

- يقصّ المعلّم/ة الصّور الموجودة في المستند رقم ١.
- يخبر التّلامذة بأنّ كلّ ورقة يحملها هي عبارة عن صورة شخص، وعليه أن يخبّئها جيّدًا.
- يقرأ لهم الرّسائل الآتية، ويطلب إليهم أن يرسموا الشّخص صاحب الرّسالة الّذي يتوقّعونه (عمره، جنسه، شكله، شخصيّته، ميوله...) وأن يذكروا من منهم يقبله كصديق، ثمّ يسألهم عن سبب رسمهم له بهذه الطّريقة. وبعد أن ينهي قراءة جميع المعلومات يريهم الصّور ويسألهم: « من هو برأيكم صاحب كلّ رسالة؟ كيف عرفتم؟ لِمَ برأيكم يقوم بعض الأشخاص بانتحال شخصيّات مزيفة على الإنترنت؟».

- الهدف من هذا النّشاط أن يعرف التّلميذ/ة أنّه ليس بالضّرورة أن يكون من نتحدّث إليه على الإنترنت الشّخصيّة الّتي يدعيها.

- **الرّسالة الأولى:** « يلّي بيعرفوا، سقراط ما بيعرفو! ويلّي بيفهموا، أنشتاين ما بيفهموا! عرفتوا مين؟ أهلي! ولو! بدا تنين يحكو فيا». أنا حاسّي حالي وحيدة، وبدّي رفيق يفهمني ويساعدني. ما حدا عم يفهمني، أهلي بيضلّوا يخانقوني، وشو ما بعمل ما بيعجبن. بتقبل تعملّي add ؟

- **الرّسالة الثّانية:** «شحّاد حاطط قدامو طبقين تيجمع فيهم مصاري، سألو واحد: مش مكفّيك طبق واحد؟ ردّ الشّحاد: أنا شفت الشّغل ماشي تمام قلت لازم إفتح فرع تاني»، أنا رامي كابتن فريق الفوتبول بمدرستي، وهوايتي المفضلة خبّر نكت وحضّر مقالب. لاحظت من تعليقاتك إنّك كتير مهضوم، شو رأيك تعملّي add ؟

- **الرّسالة الثّالثة:** «عشقي أن أعشق ويلين قلبي ويرق» ، بعرف إنّي حلوة وبلفت الأنظار، بس عم فتّش عمين يلفتلي قلبي. هوايتي كتابة الشّعر والسّباحة، حسّيت إنّو في بيناتنا شي مشترك، شو رأيك نتعرّف على بعضنا أكتر؟»

- **الرّسالة الرّابعة:** «خمس أشياء عملتا، ومن يومتا أهلي ما بيرفضولي طلب! بتحب تعرفن؟ ، أنا بحبّ الرّيّاضة، وموسيقى ال «Rap» ، وأتعرّف على ناس جداد، وتبيّنلي إنّو عندك نفس الاهتمامات، شو رأيك تعملّي add ؟»

- في حال توافرت أدوات عرض للفيديو يعرضه المعلّم/ة، ويسأل التّلامذة عمّا ينتظرونه من موضوع الحصّة.

مرحلة التّعلّم (٣٠ دقيقة):

النّشاط الأوّل:

كلّ جملة واردة في المستند رقم ٢ تعبّر عن آراء حول موضوع «الغريب على الإنترنت».

- يقوم المعلّم/ة بقصّ كلّ جملة على حدة، ويطويها ويضعها في علبة.
- يوزّع الصّفّ على ثلاث مجموعات، ويطلب إلى كلّ مجموعة أن تسحب، بطريقة عشوائيّة، خمس أوراق ليصار إلى مناقشة مضمونها ضمن المجموعة (تأييد، رفض، مع تعليل).
- تعرض كلّ مجموعة أوراقها ومواقفها، ويطلب المعلّم/ة إلى بقيّة المجموعات التّدخّل وإبداء الرّأي في حال أرادوا تصحيح موقف معيّن، وفي حال لم تصل المجموعات إلى النّتيجة المطلوبة يتدخّل مباشرة.

الأجوبة المقترحة:

- **لا بأس إذا أعطيت اسمي الحقيقي لشخص تعرّفت إليه على الإنترنت لأنّه لا يعرف أين أسكن ومن أكون.**
(خطأ: الاسم معلومة شخصيّة، ويجب عدم الإفصاح عنها لأيّ شخص غريب، إذ من السّهل تحديد مكان السّكن وغيرها من المعلومات بمجرّد ذكر الاسم)

- **أستطيع أن أعطي رقم الخليوي الخاصّ بي أو بأهلي لشخص تعرّفت إليه على الشّبكة لكي يرسل إليّ رسائل نصّيّة شرط أن يكون من عمري.**
(خطأ: رقم الخليوي الخاصّ بك أو بأهلك هو معلومة شخصيّة تساعد أصحاب النوايا السّيّئة على الوصول إليك، لذا عليك أن لا تتبادل أيّة معلومات شخصيّة، ولو كانت بسيطة مع الغريب).

- **لأتأكّد من هويّة الشّخص الّذي يكلّمني على الإنترنت، أطلب إليه الظّهور على الكاميرا ويب.**
(خطأ: هذه الطّريقة تساعدك فقط على التّعرّف إلى شكله، لا إلى هويّته ونواياه وطبعه. كما تتيح للغريب أن يتعرّف إليك بطريقة شخصيّة أكثر).

- **أتعرّض لمشاكل كثيرة على الإنترنت ولا يمكنني معالجتها.**
(خطأ: فبإمكانك إبلاغ الأهل أو أي شخص راشد تثق به، مثل المعلّم/ة، والعمّ، والأخ الأكبر... كما أنّ معظم التّطبيقات لديها خدمة الإبلاغ عن إساءة. كما يمكنك مراسلة موقع حماية على العنوان الآتي: www.himaya.org والاستفادة من خدمة e-helpline).

- **كلّ الأشخاص الّذين يطلبون إليك إضافتهم إلى لائحة الأصدقاء في المواقع الاجتماعيّة، وغرف الدّردشة يفتّشون عن الحب أو يشعرون بالوحدة.**
(خطأ: لا يمكننا أن نتأكّد من نوايا الشّخص على الإنترنت. فهناك أشخاص وعصابات أصحاب نوايا سيّئة يتحايلون علينا، وينتحلون شخصيّات بهدف الوصول إلى أهدافهم).
- **أصدّ block كلّ غريب يطلب إليّ إضافته إلى لائحة الأصدقاء.** (صح).

- **لا يوجد فرق بين المعارف والأصدقاء فكلّهم أصدقاء.**
(خطأ الصّديق هو الشّخص الّذي نعرفه وجهًا لوجه، وتربطنا به علاقة صداقة في الحياة الواقعيّة. أمّا المعارف فهم الأشخاص الّذين نعرفهم في حياتنا الواقعيّة معرفة سطحيّة كالأشخاص الّذين يركبون في باص المدرسة نفسه، أو الّذين يسكنون في الحي نفسه، هؤلاء هم من معارفك. أمّا الشّخص الّذي تعرفه جيّدا وتثق به، وتحبّه، وتقضي معه أوقاتًا كثيرة فهو صديقك).

- **إذا أرسل لي أحدهم صورته يمكنني حينها أن أقابله لأنّني أعرف من يكون.**
(خطأ فبعض الأشخاص أصحاب النّوايا السّيئة يزوّرون صورهم. وحتّى لو لم يزوّروا صورهم فهذا لا يعني أنّك تعرفهم، وبالتّالي لا يمكنك التّأكّد من نواياهم).

- **إذا طلب إليّ أحدهم قبوله كصديق وكان لدي أصدقاء مشتركون معه، فلا مانع من إضافته.**
(خطأ: الشّخص الوحيد الّذي نضيفه إلى لائحة الأصدقاء هو الصّديق الّذي نعرفه وجهًا لوجه وتربطنا به علاقة صداقة في الحياة الواقعية).

- **أقبل صداقة أيّ شخص على الإنترنت، ولكن إن أزعجني أشطبه من لائحة الأصدقاء.**
(خطأ: الشّخص الوحيد الّذي نضيفه إلى لائحة الأصدقاء هو الصّديق الّذي نعرفه وجهًا لوجه).

- **قبل أن أضيف أيّ شخص إلى لائحة أصدقائي عليّ أن أتأكّد من أنّني أعرفه في حياتي الواقعيّة.** (صح).

- **إذا شعرت بعدم الرّاحة وأنا أتحدّث إلى أحدهم على الشّبكة، أترك المحادثة وأصدّه على الفور.** (صح).

- **لا بأس إذا قابلت الأشخاص الّذين تعرّفت إليهم على الإنترنت، ولكن في أماكن عامّة، مثل: المطاعم، والأندية، وإلى جانب المدرسة.**
(خطأ: لا نلتق بالأشخاص الّذين نتعرف إليهم عبر الإنترنت إلا بموافقة الأهل وحضورهم).

- **قبول صديق friend request أو رفضه مرتبط بصوره ومعلوماته الشّخصيّة الّتي كتبها على الفايسبوك (عمر، جنس، دين...).**
(خطأ: الشّخص الوحيد الّذي نضيفه إلى لائحة الأصدقاء هو الصّديق الّذي نعرفه وجهًا لوجه لأنّه يمكن لأيّ شخص الإدعاء بصفات لا يمتلكها).

- **أحدهم يلاحقني باستمرار ويرسل إليّ رسائل مزعجة وغير مرغوب بها، أطلب إليه التّوقّف وأصدّه في كلّ مرّة.**
(خطأ: أبلّغ عنه من طريق خدمة الإبلاغ عن الإساءة report abuse الموجودة في معظم التّطبيقات، وأبلّغ عنه أيضًا شخصًا راشدًا أثق به، وأحفظ الرّسائل كدليل).

في نهاية النّشاط يتمّ عرض اللّوحة الجداريّة وقراءتها.

النّشاط الثّاني:

- يوزّع المعلّم/ة على المجموعات وثيقة عمل ١ ويطلب إلى كلّ مجموعة إكمال الجدول بما يناسب ليُصار الى مناقشة الأجوبة وتعليلها لاحقًا.

مرحلة التّطبيق (١٠ دقائق):

- يختار المعلّم/ة أحد الأنشطة لتنفيذه:

– **النّشاط الأوّل:** وثيقة الالتزام.

– **النّشاط الثّاني:** يطلب المعلّم/ة إلى كلّ مجموعة أن تؤلّف سيناريو، وتأخذ دور شخص غريب يحاول إقناع أحدهم بإضافته إلى لائحة الأصدقاء، ثمّ استدراجه ليفصح عن معلومات شخصيّة بهدف ترتيب لقاء. المجموعة الّتي تقدّم السّيناريو الأكثر إقناعًا تربح.

مستند رقم ١



مستند رقم ٢

لا بأس إذا أعطيت اسمي الحقيقي لشخص تعرّفت إليه على الإنترنت لأنّه لا يعرف أين أسكن ومن أكون.
أستطيع أن أعطي رقم الخليوي الخاصّ بي أو بأهلي لشخص تعرّفت إليه على الشّبكة لكي يرسل إليّ رسائل نصّيّة شرط أن يكون من عمري.
لأتأكّد من هويّة الشّخص الّذي يكلّمني على الإنترنت، أطلب إليه الظّهور على الكاميرا ويب.
أتعرّض لمشاكل كثيرة على الإنترنت ولا يمكنني معالجتها.
كلّ الأشخاص الّذين يطلبون إليك إضافتهم إلى لائحة الأصدقاء في المواقع الاجتماعيّة، وغرف الدّردشة يفتّشون عن الحب أو يشعرون بالوحدة.
أصدّ block كلّ غريب يطلب إليّ إضافته إلى لائحة الأصدقاء.
إذا أرسل لي أحدهم صورته يمكنني حينها أن أقابله لأنّني أعرف من يكون.
إذا طلب إليّ أحدهم قبوله كصديق وكان لدي أصدقاء مشتركون معه، فلا مانع من إضافته.
أقبل صداقة أيّ شخص على الإنترنت، ولكن إذا أزعجني أشطبه من لائحة الأصدقاء.
قبل أن أضيف أيّ شخص إلى لائحة أصدقائي عليّ أن أتأكّد من أنّني أعرفه في حياتي الواقعيّة.
إذا شعرت بعدم الرّاحة وأنا أتحدّث إلى أحدهم على الشّبكة، أترك المحادثة وأصدّه على الفور.
لا بأس إذا قابلت الأشخاص الّذين تعرّفت إليهم على الإنترنت، ولكن في أماكن عامّة، مثل: المطاعم، والأندية، وإلى جانب المدرسة.
قبول صديق friend request أو رفضه مرتبط بصوره ومعلوماته الشّخصيّة الّتي كتبها على الفايسبوك (عمر، جنس، دين...).
أحدهم يلاحقني باستمرار ويرسل إليّ رسائل مزعجة وغير مرغوب بها، أطلب إليه التّوقّف وأصدّه في كلّ مرّة.

وثيقة عمل ١

وصف السّيناريو	هل توجد مجازفة؟	كيف تتصرّف؟
لقد رأى صديقي، وهو مصوّر إعلانات، صورتك وأعجبته جدًّا! ما رأيك بأن تتعارفا من أجل تصوير إعلان؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
أرني كيف تبدو عليك ثياب السّباحة الجديدة الّتي اشتريتها؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
وأنا أيضًا أشجّع المانشستير! عندي صور وقمصان موقّعة من أعضاء الفريق، أين تسكن لأرسل إليك صورة وقميصًا؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
إذا لم توافيني بعد ساعة فسوف أنشر الصّورة الّتي أرسلتها لي!	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
– سيّارة رائعة! – شكرا! ما رأيك أن أقلّك بها إلى البيت بعد المدرسة؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
بعد قليل سيفرغ رصيد خدمة الإنترنت، فلنكمل حديثنا على الخليوي، ما هو رقمك؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
والداي متشدّدان جدًّا! فلنلتق عند السّاعة العاشرة مساء في مكان حيث لا يمكن أن يرانا أحد.	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
أبي أيضاً مدرس فيزياء! في أي مدرسة يدرّس والدك؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
أريد أن أتعلّم كرة السّلة، بأيّ نادٍ تنصحني؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
أحبّ أن أتمشّى على المارينا، وأنت ما هو مكانك المفضّل؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
الطّقس حارّ جدّا اليوم، كم تبلغ درجة الحرارة عندك؟	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث
إذا زرت الموقع الفلاني سوف تجد أجوبة عن سؤالك! وسوف تذهل لما ستراه!	☐ نعم ☐ كلا	☐ أستمرّ بالمحادثة ☐ أقطع المحادثة ☐ أبلّغ شخصًا راشدًا أثق به ☐ أصدّ المتحدث

وثيقة الالتزام

أ – أملأ الفراغ بالكلمات المناسبة.
ب – أضع علامة × داخل المربّع المقابل لكلّ التزام وافقت عليه:

انتحال – الشّخصيّة – الإساءة – خطئي – مزيّفة – مزعجة – شخصيّة – وحدي – مقابلة – حقيقيّة – أخبر – أردّ – يزعجني – أتحدّث.

ليس بالضّرورة أن يكون من نتحدّث إليه على الإنترنت.. الّتي يدعيها، فقد يكون منتحلا شخصيّة أخرى بصورة .... وعمر مزيف، لذلك:

☐ لن .... مع الغرباء على الإنترنت، لأنّه من السّهل .... شخصيّة غير .... بغرض .... إلي.

☐ أنا أرفض .... أيّ شخص تعرّفت إليه على شبكة الإنترنت من دون استشارة أهلي أو شخص راشد أثق به. وفي حال موافقتهم، لن أقابله .... بل بوجودهم أو بوجود شخص راشد معي.

☐ أنا .... دائما شخصا راشدا أثق به عن أيّ شيء أو أيّ شخص .... على الإنترنت.

☐ أنا لن أفصح عن أيّة معلومات .... عنّي أو عن أهلي لأيّ شخص على الشّبكة.

☐ انا أعلم أنّه ليس من .... إذا وصلتني رسائل .... وأنا لن ...... عليها ....

أنا الموقّع أدناه... أتعهّد بالوفاء بما التزمت به لكي أعيش تجربة آمنة ومسلّية على الشّبكة.

التّاريخ... التّوقيع...

٣- الغريب على الانترنت

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتمكّن من المحافظة على المعلومات الشّخصيّة والتّواصل الآمن عبر الإنترنت.

الموارد:

- يتعرّف إلى مفهوم الغريب.
- يعي بعض مخاطر التّواصل مع الغريب عبر الإنترنت.
- يتعرّف إلى بعض القواعد الأساسيّة للتّواصل الآمن مع الغريب عبر الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهيّة الغريب. • طرق الحماية على الشبكة.	• يفرّق بين مفهوم الأصدقاء والمعارف. • يفرّق بين العلاقات الواقعيّة والافتراضيّة. • يفرّق بين الصّفحة الحقيقيّة والصّفحة الوهميّة Real & Fake Profile.	• يرفض التحدّث إلى الغرباء على الإنترنت أو مقابلتهم شخصيًّا. • يقطع أيّة محادثة أو دردشة لا توحي بالرّاحة. • يخبر شخصًا راشدًا، يثق به، عن أيّ شيء أو شخص يزعجه على الإنترنت.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص:٨-٩-١٠-٢٣-٢٦، اللّوحة الجداريّة «الغريب online ممكن يكون خطر offline»، فيديو «الغريب» فيديو المواطنيّة الرّقميّة.
- **نمط التّنفيذ:** عمل فردي، عمل ضمن مجموعات، نقاش.
- **المكان:** الصّفّ.

سير النّشاط:

التّحفيز (٧ دقائق):

- في حال توافرت أدوات عرض للفيديو يقوم المعلّم/ة بعرضه ويسأل التّلامذة عمّا ينتظرونه من موضوع الحصّة.
- يطلب المعلّم/ة إلى التّلامذة أن يسمّوا بعض التّطبيقات، والبرامج الموجودة على الإنترنت أو الأجهزة الالكترونيّة الخاصّة بالتّواصل الاجتماعي، وأن يخبروه عن ميزات كلّ منها (فايسبوك، سكايب، واتس آب...).
- ثمّ يطلب إليهم أن يكتبوا على ورقة مستطيلة بيضاء محتوى رسالة أرسلها إليهم شخص لا يعرفونه على الإنترنت ليطلب إليهم إضافته إلى لائحة الأصدقاء (على المعلّم/ة أن يحترم خصوصيّتهم، ويطلب إليهم ألّا يذكروا أسماءهم) ثمّ يجمع الأوراق في علبة.

مرحلة التّعلّم (٣٣ دقيقة):

- يوزّع المعلّم/ة التّلامذة على مجموعات، ويعطي كلّ مجموعة ورقة كرتون كبيرة رُسمَ عليها دائرة وكُتبَ بداخلها إحدى العبارات الآتية: « فايسبوك شبكة تعارف»، « قواعد الدّردشة الآمنة علىَ الإنترنت»، «طلَب إضافة صديق Friend Request»، « أريد أن ألتقي وجهًا لوجه بصديق تعرّفت إليه عبر الإنترنت».
- يطلب المعلّم/ة إلى كلّ تلميذ/ة في المجموعة أن يدوّن تعليقًا على الكرتونة (قد يكون هذا التّعليق مرتبطًا بالعبارة الموجودة أصلًا عليها أو ردًّا على تعليقات رفاقه).
- عند إشارة المعلّم/ة، تتبادل المجموعات الكراتين، ويتكرّر العمل نفسه حتّى تمرّر الكراتين على المجموعات جميعها. وعند الانتهاء يقرأ أحد أفراد كلّ مجموعة خلاصة ما كتب على الكرتونة الموجودة معه.
- بعد الانتهاء، يجمع المعلّم/ة الكراتين، ويرسم على اللّوح الجدول الآتي:

إيجابيّات شبكات التّواصل الاجتماعي	سلبيّات شبكات التّواصل الاجتماعي	قواعد التّواصل الآمن على الإنترنت

- يقرأ المعلّم/ة إجابات التّلامذة ويملأ الجدول.

ملاحظة:
يمكن للمعلّم مقارنة القواعد المدوّنة على اللّوح بتلك الموجودة في اللّوحة الجداريّة.

- يخبر المعلّم/ة التّلامذة أن المتحرّشين والمحتالين يستخدمون طرقًا عدّة للإيقاع بضحاياهم، ويطلب إليهم أن يذكروا هذه الطّرق ويدوّنوها على اللّوح (التّعاطف أي عندما يعكس المتحرّش حالة الولد على نفسه. مثلًا: إذا كان الولد يشعر بالوحدة يخبره أنّه يمرّ بالحالة نفسها، أو إذا كان يحبّ موسيقى معيّنة يخبره أنّه يحبّها أيضًا، المديح أو الغزل، الوعود، التّهديد...) ويطلب إليهم أن يقدّموا أمثلة.

- يقرأ المعلّم/ة الأوراق الّتي جمعها في علبة، ويحاول، بالتّعاون مع التّلامذة، تصنيفها شفهيًّا ضمن الطّرق الّتي ذكرت.

مرحلة التّطبيق (١٠ دقائق):

- يوزّع المعلّم/ة على كلّ مجموعة قصّة تحوي جزءًا ناقصًا ويطلب إلى كلّ منها أن يكملوا الجزء النّاقص من القصّة:

قصّة١:

«يا صاحبة العينين العسليّتين، أشفقي على قلبي بكلمة»، قرأت جينا هذه الرّسالة الّتي وصلتها على الفايسبوك من شخص يستخدم «عاشق ولهان» كـ «إسم مستخدم». إنّه فارس أحلامها، فهو شاب أسمر ذو عينان زرقاوتان. ولكنّها انتبهت لوجود والدتها إلى جانبها تشاهد مسلسلها المفضّل على التّلفاز.
قالت لأمّها: «لقد أصابني النّعاس، تصبحين على خير يا أمي» وحملت جينا معها المحمول وذهبت إلى سريرها
....

تعلمت جينا درسًا قاسيًا من هذه الحادثة وتذكّرت كلمات أمّها: «ليس كلّ ما يلمع ذهبًا».

قصة٢:

«أنا وحيدة أبحث عن الصّداقة، هل تودّ أن تكون صديقي» قرأ رامي هذه الرّسالة وبدأ بطباعة هذه الكلمات على الشّاشة: «بالطّبع وأنا أيضًا بحاجة إلى رفيقة أشكو لها همّي». همّه كبير فأبوه وأمّه غير متّفقين فهو يستيقظ على صراخهما، وينام على صوت بكاء أمّه أو صراخ والده. ....
....

سأله والده: هل تشعر الآن بالتّحسن؟ يوجد شرطي على الباب يريد أن يأخذ إفادتك»، فأجابه رامي: «فليدخل». دخل الشّرطي، وألقى التّحيّة على الموجودين ثمّ هنّأه على سلامته وسأله: «هل تعرّفت إلى أحدهم فأجابه رامي: «كانوا عدّة أشخاص ملثّمين، والظّلام دامس، لم أتعرّف إلى أحد».

قصّة ٣:

« أمّي! أرسل أحدهم لي رسالة، يقول إنّ اسمه ريان، ووالده من قريتنا، وهو يحمل شهرتنا نفسها، ويطلب إليّ أن أضيفه إلى لائحة الأصدقاء»، أجابت أمّ جاد: «اسأله ابن من هو؟ فلنتأكّد من صوره. هذا أبوه، وهذه أمه. لقد كانت رفيقتي في المدرسة، اطلب إليه أن يفتح الويب كاميرا كي أتحدّث مع أمّه إذا كانت موجودة». . . . .
. . . .

غادر ريان لبنان عائدا إلى بلاد الغربة، ولكنّه لن ينسى صديقه جاد وعائلته الّتي اهتمت به اهتماما بالغا حيث قضى أفضل الأوقات برفقتهم. وعلى الرّغم من المسافات الّتي تفصل بينهما فإنّ الإنترنت قرّبها، وما زالا من أعزّ الأصدقاء يتواصلان باستمرار.

قصّة ٤:

رامي وجينا صديقان منذ الطّفولة، كانا يسكنان في منزلين مجاورين، ويرتادان المدرسة نفسها، لا يفترقان أبدا. وفي يوم من الأيّام، جاء رامي والحزن باد على وجهه، فسألته جينا: «ما بالك يا رامي؟ تبدو حزينًا جدًّا! هل من مشكلة؟»، أجابها رامي: « لقد عُيّن والديً مديرًا لفرع من فروع الشّركة الّتي يعمل بها، راتب مغر، وفرصة عمل لا تعوّض! ولكنّ هذا الفرع موجود في أفريقيا، وبعد أسبوع سنغادر لبنان!» واغرورقت عيناهً بالدّموع.
. . . .

«حقا يا جينا! لقد كنت خير رفيقة لي! لقد ساعدتني في تخطّي جميع الصّعوبات الّتي مررت بها في عالم الاغتراب وكأنّك معي! وعلى الرّغم من المسافات الّتي كانت تفصل بيننا فإنّ الإنترنت قرّبها. وها نحن الآن معا تحت سقف واحد! لقد استيقظ ابننا رالف وهو يصرخ، يبدو أنّه جائع!».

لقد وصلني بريد إلكتروني، يفيد أنّني ربحت جائزة ماليّة كبرى. وللحصول عليها يجب أن أدخل بعض المعلومات الشّخصيّة فقط.

ولكنّك لم تشترك في أيّة مباراة. فكيف لك أن تربح؟!

أنا أحمي حاسوبي الشخصي:

- أنا أستخدم البرمجيات المضادة للفيروسات وأحدّثها دوريًا.
- أنا أتجاهل وأحذف الرّسائل البريديّة المزعجة أو المجهولة المصدر.
- أنا أحصّن كلمة السرّ باستخدام ثمانية أرقام على الأقل تجمع ما بين الحروف والأرقام والرموز وأقوم بتغييرها بشكل دوري.
- أنا لن أحمّل الملفّات (download) أو أنقر على الوصلات (links) أو الملحقات (attachment) إلاّ في حال كنت أثق بالمصدر أو أستشير أحدًا ما.



البرمجيّات الخبيثة والخداع

١- أنا أحمي حاسوبي!

الكفاية الأولى: في نِهاية مرحلة التّعليم الأساسي ، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتعرّف إلى البرمجيّات الخبيثة والخداع والاحتيال على الشّبكة، وكيفيّة حماية الأجهزة والمعلومات.

الموارد:
- يتعرّف إلى ماهية الخداع.
- يتعرّف إلى ماهية البرمجيّات الخبيثة، وتأثيرها على الحاسوب والبيانات.
- يتعرّف إلى بعض القواعد العامّة لتفادي الوقوع ضحيّة الخداع والاحتيال والبرمجيات الخبيثة.

المعارف	المهارات والقدرات	المواقف
• ماهيّة الخداع. • ماهيّة البرمجيّات الخبيثة. • ماهيّة القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة.	• يطبّق قواعد حماية الكمبيوتر من البرمجيات الخبيثة. • يطبّق القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة. • يكتب كلمة سرّ محصّنة بمساعدة شخص راشد.	• يستشير شخصًا راشدًا لتحميل الملفّات أو النّقر على الوصلات(links) أو الملحقات (attachments) • يتجنّب فتح أيّ بريد الكتروني من شخص أو مصدر غير معروف. • يرفض تحويل أيّة رسائل واردة إلى بريده للآخرين دون استشارة شخص راشد. • يرفض الرّدّ على أيّة رسالة إلكترونيّة يطلب فيها إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة. • يرفض الاستجابة للعروض الوهميّة المغرية (جوائز...).

- **الفئة المعنيّة:** تلامذة الصّفّين الرّابع والخامس من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٥...٢٢-٢٤-٢٥، مطويّة الأطفال، وثيقة عمل ١، ورقة عمل «أتخيّل وأرسم».
- **نمط التنفيذ:** عمل مجموعات، نقاش.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (٧ دقائق):

- يختار المعلّم النشاط الأوّل أو النشاط الثاني:

النشاط الأوّل:

- يخبر المعلّم/ة تلامذته أنّهم سيجرون سحبًا بالقرعة، وعلى كلّ مشترك أن يدفع مبلغ ألف ليرة لبنانيّة للاشتراك بها والفائز سوف يربح جهاز I-pad.

- يضع المعلّم/ة أسماء المشتركين في المسابقة في علبة ويسحب ورقة عشوائيّة، لكن لا يقرأ الاسم المكتوب فيها بل يقرأ اسم تلميذ/ة غير مشترك في المسابقة أو اسم تلميذ/ة من صفّ آخر. ويستمع إلى احتجاجاتهم (مثلًا: التّلميذ الفلاني لم يشترك في المسابقة. وكيف ربح؟ عندها أخبرهم: أنّ الشّيء نفسه ينطبق على عالم الإنترنت والخليوي أيضًا، إذ تصلكم رسائل تفيد أنّكم ربحتم جائزة وأنتم لم تشتركوا فيها أصلًا، وهذا ما نسمّيه الخداع).

النشاط الثاني:

- يطلب المعلّم إلى التّلامذة أن يحلّوا الجزء الأوّل من وثيقة عمل ١، ويتوقّعوا موضوع الحصّة.

مرحلة التعلم (٣٣ دقيقة):

- يُوزّع المعلّم/ة التّلامذة إلى أربع مجموعات، ويعطي كلّ مجموعة ورقة كرتون كبيرة عليها إحدى الصّور الموجودة في وثيقة عمل ١.

- يطلب إلى كلّ تلميذ/ة في المجموعة أن يدوّن تعليقًا على الورقة (قد يكون هذا التّعليق مرتبطًا بالعبارة الموجودة أصلا على الورقة أو ردّا على تعليقات رفاقه).

- عند إشارة المعلّم/ة، تتبادل المجموعات الأوراق، وتكرّر العمليّة نفسها حتّى تمرّر الأوراق على المجموعات جميعها.

- لتوجيه النّشاط بطريقة أكثر فعاليّة، يمرّ المعلّم/ة بين التّلامذة ويطرح عليهم أسئلة توضيحيّة. على سبيل المثال:
  - لمَ تعتقدون أن الحاسوب أصبح على هذه الحالة؟
  - مَا هي الأمور الّتي نقوم بها وتجعل الحاسوب يبدو مريضًا في هذه الصّورة؟
  - ما موضوع الصّورة الثّالثة؟ ماذا يحصل فيها؟

– ماذا يعني هروب الحاسوب؟
– لِمَ يركض اللّصّ؟ وماذا سرق؟ ما هي الأمور الّتي قام بها الرّجل وأدّت إلى هذه النّتيجة؟

- بعد أن ينهي الصّفّ عمله، يكتب المعلّم/ة على اللّوح: كيف أحمي حاسوبي ومعلوماتي الشّخصيّة على الإنترنت؟ ويطلب إلى كلّ مجموعة قراءة المعلومات الموجودة على الورقة الّتي أمامها ليصار إلى استنتاج قواعد حماية الحاسوب والمعلومات الشّخصيّة فيدوّنها على اللّوح (من دون ذكر النّقاط الّتي لم يتطرّقوا إليها).

- يطلب المعلّم/ة إلى التّلامذة أن يعملوا بشكل مجموعات رباعيّة، ويوزّع على كلّ مجموعة وثيقة عمل ١ (نسخة واحدة عن الورقة الأولى من الوثيقة، وأربع نسخ عن الورقة الثّانية من الوثيقة لكلّ مجموعة، والسّبب أن بعض الجمل تؤدّي إلى أكثر من نتيجة).

- يطلب المعلّم/ة إلى المجموعات قصّ الصّور الأربع والجمل الموجودة في وثيقة عمل ١، ولصق كلّ صورة على ورقة بيضاء مع النّتيجة المناسبة لها. ويسألهم: هل هناك من نقاط لم تذكر على اللّوح؟ ما هي؟ ويقوم بتدوينها.

ملاحظة:
يمكن المعلّم/ة الاستفادة من النّقاط الموجودة في مطويّة الأطفال والأهل، والمادّة التدريبية في ما يتعلّق بقواعد حماية الحاسوب والمعلومات الشّخصيّة.

مرحلة التّطبيق (١٠ دقائق):

ورقة عمل «أتخيّل وأرسم».

أتخيّل وأرسم

أتخيّل ثمّ أرسم داخل المربّع:

لو كان فيروس الحواسيب حيوانًا ، لكان يشبه:

لو كان فيروس الحواسيب شيئًا، لكان يشبه:

لو كان فيروس الحواسيب إنسانًا، لكان يشبه:

لو كان الاحتيال على الإنترنت حيوانًا، لكان يشبه:

لو كان الاحتيال على الإنترنت شيئًا لكان يشبه:

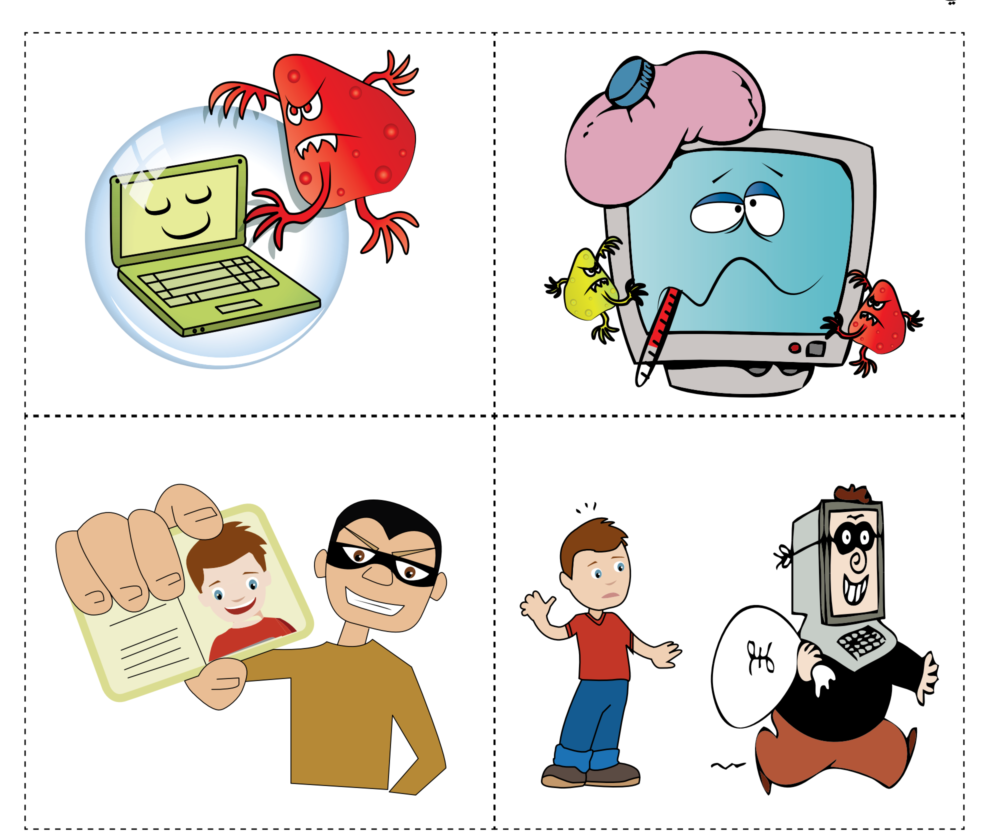
لو كان الاحتيال على الإنترنت إنسانًا، لكان يشبه:

وثيقة عمل ١

الجزء الأوّل: أضع نفسي مكان رانيا، وأكتب لسامي ردًّا مناسبًا في الغيمة الثّانية.



الجزء الثاني:



- أقصّ الجمل الآتية ، وألصقها على الورقة الّتي تحمل الصّورة المناسبة للنّتيجة:

أنا أحصّن كلمة السّرّ باستخدام ٨ رموز على الأقلّ تحوي حروفًا وأرقامًا ورموزًا .
لا أستخدم كلمات مرور مختلفة لكي لا أنساها .
أنا أستخدم البرامج المضادة للفيروسات Anti–Virus .
أنا أُحدّث update البرنامج المضاد للفيروسات مرّة كلّ شهرين .
أنا أفتح أيّ بريد الكتروني مرسل من شخص لا أعرفه ، وإن لم تعجبني الرّسالة أغلقها .
أنا أردّ على بعض الرّسائل الالكترونيّة الّتي يُطلب فيها إعطاء معلومات شخصيّة .
انا أختار اسم مستخدم وكلمة مرور لا يكشفان عن أيّة معلومات ماليّة أو شخصيّة تخصّني .
أنا أحمّل الألعاب والأغاني المجانيّة الّتي أحبّها من مختلف المواقع .
إن ظهرت رسالة مفادها أنّي فزت بجائزة ، أنقر عليها فلن أخسر شيئًا بل ربّما أربح .
أنا لا أتصفّح الحسابات الخاصّة الّتي تتطلّب كتابة كلمة المرور مثل الفايسبوك ، والبريد الإلكتروني على أجهزة الكمبيوتر العامّة في المدرسة ، والمكتبة ، ومقاهي الإنترنت .

٢- أنا ذكيّ على الشّبكة!

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتعرّف إلى البرمجيّات الخبيثة والخداع والاحتيال على الشّبكة، وكيفيّة حماية الأجهزة والمعلومات.

الموارد:
- يتعرّف إلى أساليب الخداع والاحتيال الأكثر شيوعًا.
- يتعرّف إلى أنواع البرمجيّات الخبيثة الأكثر شيوعا وتأثيرها على الحاسوب والبيانات.
- يتعرّف إلى القواعد الأساسيّة لتفادي الوقوع ضحيّة الخداع والاحتيال والبرمجيّات الخبيثة.

المعارف	المهارات والقدرات	المواقف
• أساليب الخداع والاحتيال الأكثر شيوعًا. • ماهيّة البرمجيّات الخبيثة. • القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة.	• يحدّد أهم أنواع وأساليب الخداع والاحتيال الموجودة على الإنترنت e-mail ،phishing ،scams ،spoofing. • يحدّد أهمّ أنواع البرمجيّات الخبيثة الموجودة على الإنترنت (الفيروس virus، حصان طروادة Trojan horse، الدّيدان worms...) • يطبق القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة. • يكتب كلمة سرّ محصّنة. • يستخدم البلوتوث والواي فاي بشكل آمن Blue Tooth و WiFi.	• يستشير شخصًا راشدًا قبل تحميل الملفّات أو النّقر على الوصلات (links) أو الملحقات (attachments). • يتجنّب فتح أو كتابة ردّ على بريد الكتروني أو رسالة مرسلة من مصدر غير معروف. • يرفض تحويل رسائل واردة إلى بريده للآخرين من دون التمعّن في محتواها والجهة الواردة منها. • يرفض الرّدّ على أيّة رسالة الكترونيّة يطلب فيها إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة. • يهمل العروض الوهميّة المغرية.

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص:١٥...٢٢-٢٤-٢٥، ورقة عمل «رانيا تخدع»، ورقة عمل ١ وثيقة عمل «لعبة التّعريفات»، مطويّة الأطفال، فيديو البرمجيّات الخبيثة وفيديو المواطنيّة الرّقميّة.
- **نمط التنفيذ:** عمل مجموعات، نقاش.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق):

- يطلب المعلّم/ة إلى التّلامذة أن يضعوا أمامهم ورقة وقلمًا، ويخبرهم أنّه سيجري لهم امتحانًا، وسوف يعطي علامات إضافية لكلّ من ينجح فيه.

- يطرح المعلّم/ة على التّلامذة أسئلة سهلة ليجيبوا عنها. على سبيل المثال:
  - ما هي عاصمة لبنان؟
  - إذا كان لديك ١٠ تفاحات وتريد أن توزّعهم على خمسة تلامذة، فكم تفاحّة تعطي لكلّ تلميذ؟
  - ما هو الشّيء الّذي نشربه ونجده في البحر، وفي الغيوم؟
  - ألّف جملة تبدأ بكلمة «ذهب».
  - أذكر جهازين نستخدم فيهما الإنترنت.

- بعد أن يجيب التّلامذة عن الأسئلة، يخبرهم المعلّم/ة أنّه ألغى المسابقة. وعندما يسأله التّلامذة: لماذا؟ يخبرهم أنّها مزحة ويسألهم: ألم تلاحظوا أنّ الأسئلة سهلة جدًّا؟؟ فكيف صدّقتم؟

- يدوّن المعلّم/ة على اللّوح العبارات الآتية: «جوائز على الإنترنت!»، «حاسوبي محصّن!» ويترك مجالًا ليكتب التّلامذة تعليقاتهم على اللّوح (قد يكون هذا التّعليق مرتبطًا بالعبارة الموجودة أصلا على اللّوح أو ردًّا على تعليقات رفاقه).

- ثمّ يسألهم عما ينتظرونه من الحصّة.

مرحلة التعلم (٣٣ دقيقة):

- يوزّع المعلّم/ة التّلامذة إلى مجموعات ويطلب إلى كلّ مجموعة تنفيذ نشاط «لعبة التعريفات» (في حال وجود الإنترنت يسمح لهم المعلّم/ة باستخدامه لحلّ التّمرين).

- يطلب المعلّم/ة إلى كلّ تلميذ أن يقرأ ورقة عمل «رانيا تخدع» بصمت، ثمّ تتمّ مناقشة مضمونها ضمن المجموعات ليصار لاحقًا إلى الإجابة عن الأسئلة المطروحة فيها شفويًا.

- **لمحة مساعدة للمعلّم عن قصّة رانيا:** لم تتأكّد رانيا قبل طباعة كلمة المرور من أنّ الرّسالة آتية من موقع آمن أي وجود https على الرّابط. كما وأنّها لم تنتبه إلى أنّ اسم الموقع مكتوب بطريقة غير صحيحة fakebok. بالإضافة إلى أنّها لم تنتبه أنّه في المواقع الآمنة لا تظهر أبدًا كلمة المرور عندما نطبعها بل تكون مشفّرة، وهذا ما أدّى إلى وقوعها ضحيّة سرقة حسابها على الفايكبوك. وبما أنّها استخدمت كلمة المرور نفسها لبريدها الالكتروني فقد سُرِقَ، وعبث السّارق بصورها ورسائلها وانتحل شخصيّتها، وهذا ما نسمّيه سرقة الهويّة.

- يطرح المعلّم/ة سؤالا: هل يودّ أحدكم إضافة تعليقات أخرى على ما دُوِّنَ سابقًا على اللّوح؟ (في حال كانت الإجابة «نعم» تتمّ إضافة التّعليقات الجديدة).

ملاحظة:
يمكن المعلّم/ة الاستفادة من النّقاط الموجودة في مطويّة الأطفال والأهل، والمادّة التّدريبيّة في ما يتعلّق بمحتوى النّشاط.

التّطبيق (١٠ دقائق):

ورقة عمل ١ (في حال توافر أدوات لعرض الفيديو يتمّ عرضه من باب التّذكير).

بينما كانت رانيا تستخدم الفايكبوك، ظهرت رسالة طارئة تطلب إليها إعادة كتابة كلمة المرور.
لو كنت مكان رانيا، كيف تتصرّف؟

....

....

....

....

ما هو الخطأ الأوّل الّذي ارتكبته رانيا وأدّى إلى سرقة حسابها على الفايكبوك؟

....

....

لماذا سُرق بريدها الإلكتروني أيضًا؟

....

....

تخيّل بعض الأفعال الّتي يمكن أن يكون قد قام بها السّارق ووضع رانيا في مواقف حرجة؟

....

....

....

....

....

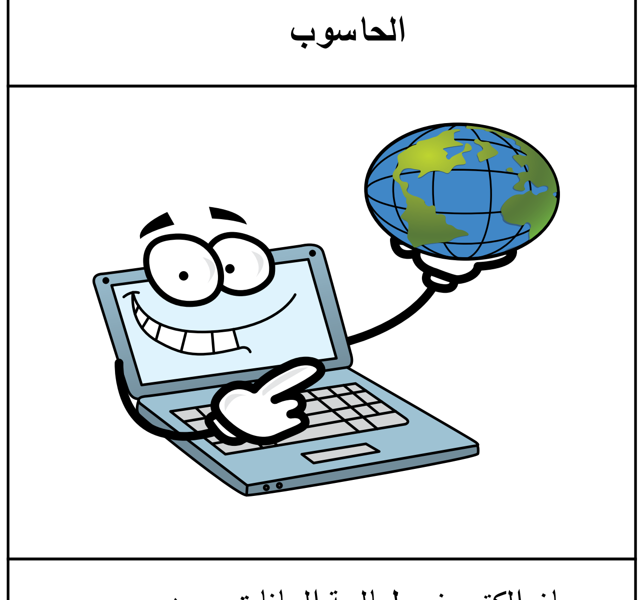
اذكر بعضًا من المحتوى الّذي يمكن أن تكون قد وضعته رانيا على حساب الفايكبوك والّتي تتيح للسّارق فرصة استغلاله أو تشويهه للإساءة إليها.

....

....

الصق المصطلح والصّور المناسبة لكلّ تعريف متّبعًا المثال:

مثلاً:

الحاسوب

جهاز الكتروني لمعالجة البيانات، وهو قادر على إجراء عدد هائل جدًّا من العمليّات الحسابيّة والمنطقيّة في زمن قياسيّ.

Spyware	Trojan Horse	Adware
Virus	Worms	Spam
Firewall	Scam	Pop-Up
Anti-virus	Chain e-mail	Identity theft


أنضم
الآن
أكثر من ١،٠٠٠،٠٠٠
مشارك
جهازك
بطيء؟
٧٠٪ حسم
حدد السعر الذي تريد
للجادين فق
نقل مجا
إضغط هنا
وأربح رحلة!
عرض مغري
مبروك!
لقد ربحت
جرّب الآن
مجاناً
إشتري الآن
BOOM!

برنامج يعرض الإعلانات بصورة مستمرّة.	برنامج خبيث يقوم بإدراج نفسه داخل ملفّ، ويهدف إلى تعطيل العمل في الكمبيوتر، ولكنّه لا يستطيع مضاعفة نفسه.
بريد الكتروني خادع يطلب إلى مستلمه أن يمرّره إلى أشخاص عدّة بحجّة ما. مثل: مساعدة إنسانيّة أو نصائح طبّيّة...	انتحال هويّة شخص ما، وذلك من طريق سرقة معلوماته الشّخصيّة من دون علمه عن الإنترنت، من أجل سرقة المال أو القيام بجريمة أخرى، وهي جريمة يعاقب عليها القانون.

برنامج خادع ويبدو كأنّه مفيد، ولكنّه بالحقيقة يهدّد أمن الكمبيوتر ويتسبّب بالأضرار.	بريد مزوّر يُظهِر أنّ المرسل هو شخص ذو منصب معيّن كمدير شركة أو بنك أو من فريق صيانة موقع معروف مثل hotmail، facebook، ويطلب إلي المستخدم معلومات عن حسابه متذرّعًا بحجّة ما أو حالة طارئة. فينخدع المستخدم بذلك ويستجيب لطلبه.

برنامج أو جهاز يساعد في منع المتطفّلين أو البرامج الخبيثة من الوصول إلى الكمبيوتر من خلال إحدى الشّبكات أو الإنترنت.	نوافذ دعائيّة تنبثق وترافق بعض الصّفحات، وتزعج المستخدم.

برنامج ضار يقوم بمضاعفة نفسه من خلال الإنترنت، وينتقل من جهاز إلى آخر.

برنامج يُستخدم لاكتشاف البرمجيّات الخبيثة، ومنعها من الوصول إلى الحاسوب والبيانات، وإزالتها عنه.

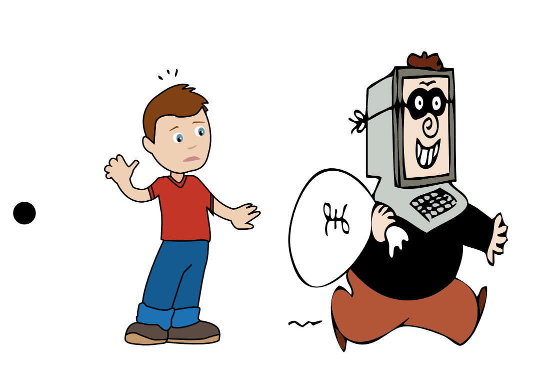
بريد الكتروني مزعج وغير مرغوب به يُرسل إليك بكمّ هائل.

برنامج تجسّسي، يتعقّب تحرّكاتك على الشّبكة العنكبوتيّة، ويعرف عنك معلومات كثيرة من دون علمك.

ورقة عمل ١

أربط كلّ جملة بالصّورة المناسبة للنّتيجة:





- أنا أحصّن كلمة السرّ باستخدام ٨ رموز على الأقل تحوي حروفًا وأرقامًا ورموزًا.
- أنا لا أستخدم كلمات مرور مختلفة لكي لا أنساها.
- أنا أُحَدّث update البرنامج المضاد للفيروسات مرّة كلّ شهرين.
- أنا أفتح أيّ بريد إلكتروني مرسل من شخص لا أعرفه، وإن لم تعجبني الرّسالة أغلقها.
- أنا أردّ على بعض الرّسائل الالكترونيّة الّتي يطلب إليّ فيها إعطاء معلومات شخصيّة أو ماليّة.
- انا أختار اسم مستخدم وكلمة مرور لا يكشفان عن أيّة معلومات ماليّة أو شخصيّة تخصّني.
- أنا أحمّل الألعاب المجانيّة الّتي أحبّها أو الملفّات من مختلف المواقع.
- أنا أنقر على كلّ رسالة تخبرني أنّني فزت بجائزة، فلن أخسر شيئًا بل ربّما أربح.
- أنا أتصفّح الحسابات الخاصّة مثل الفايسبوك، والبريد الإلكتروني، وأتسوّق على أجهزة الكمبيوتر العامّة في المدرسة، والمكتبة، ومقاهي الإنترنت.
- أنا أستخدم البرامج المضادة للفيروسات anti-virus، وأقوم بتحديثها، لذا لا داع لاستخدام جدار النّار firewall.
- أنا أمرّر فقط الرّسائل الّتي يُطلب إليّ فيها أن أرسلها إلى أشخاص عدّة بهدف التّوعية أو المساعدة.
- أنا أزوّد صديقا مقرّبًا أثق به بكلمة المرور فقط في حال كنت مضطرًّا لتصفّح حساباتي ولم يكن لديّ إنترنت.
- أنا أتأكّد من مصداقيّة الموقع من خلال فحص رابط عنوان الموقع، ووجود https عند طلب كلمة المرور، وأتأكّد من أنّها تُطبع على الشّاشة بشكل مشفّر (××××××مثلا).

٣- البرمجيّات الخبيثة والخداع على الإنترنت.

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي ، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يتعرّف التّلميذ إلى البرمجيّات الخبيثة والخداع والاحتيال على الشّبكة، وكيفيّة حماية الأجهزة والمعلومات.

الموارد:
- تعرّف إلى أحدث أساليب الخداع والاحتيال.
- يتعرّف إلى أحدث أنواع البرمجيّات الخبيثة وتأثيرها على الحاسوب والبيانات.
- يتعرّف إلى القواعد الخاصة بكل نوع من أنواع الخداع والاحتيال والبرمجيّات الخبيثة.

المعارف	المهارات والقدرات	المواقف
• أحدث أساليب الخداع والاحتيال. • ماهيّة البرمجيّات الخبيثة. • القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة.	• يحدّد أهم أنواع وأساليب الخداع والاحتيال الموجودة على الإنترنت e-mail، phishing، scams spoofing. • يحدّد أهمّ أنواع البرمجيّات الخبيثة الموجودة على الإنترنت (الفيروس virus، حصان طروادة Trojan horse، الدّيدان worms...) • يطبق القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي في مقاهي الإنترنت أو الأماكن العامّة. • يكتب كلمة سرّ محصّنة. • يستخدم البلوتوث والواي فاي بشكل آمن Blue Tooth و WiFi. • يستخدم البرامج المضادة للفيروسات، كبرامج مكافحة التّجسّس، وجدار الحماية firewall. ويحدّثها بشكل منتظم.	• يستشير شخصا راشد قبل تحميل الملفّات أو النّقر على الوصلات (links) أو الملحقات (attachments). • يتجنّب فتح أو كتابة ردّ على بريد الكتروني أو رسالة مرسلة من مصدر غير معروف. • يرفض تحويل رسائل واردة إلى بريده للآخرين من دون التمعّن في محتواها والجهة الواردة منها. • يرفض الرّدّ على أيّة رسالة الكترونيّة يطلب فيها إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة. • يهمل العروض الوهميّة المغرية.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّتان كاملتان.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٥...٢٢-٢٤-٢٥، مطويّة الأهل والأطفال، فيديو أمن البيانات.
- **نمط التنفيذ:** بحث ضمن عمل مجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (٥ دقائق):

- يطلب المعلّم/ة إلى كلّ تلميذ/ة ملء الجدول الآتي بما يناسب وذلك بعد رسمه على دفاترهم.

ماذا تعرف عن البرمجيّات الخبيثة؟	ماذا تعرف عن الخداع والاحتيال على الشّبكة؟

مرحلة التّعلّم (٨٠ دقيقة):

- يشرح المعلّم/ة محتوى المواضيع المقترحة.
- يوزّع التّلامذة على مجموعات عمل خماسيّة.
- تحدّد مهمّة كلّ مجموعة من خلال السّحب بالقرعة.
- يوزّع المعلّم/ة على كلّ مجموعة ورقة العمل الخاصّة بها، ويطلب إلى التّلامذة تحضير العمل ليصار إلى عرضه بعد مدّة محدّدة (أسبوع مثلا).

ملاحظة:
مدّة عرض كلّ مجموعة ٢٠ دقيقة فقط.

الموضوع الأوّل: البرمجيّات الخبيثة على الإنترنت:

أستاذ/ة المعلوماتيّة في مدرستكم متضايق جدًّا من الأضرار الّتي تتسبّبون بها أثناء استخدامكم الإنترنت في مختبر المعلوماتيّة. وهو يشكو باستمرار من بطء سرعة الجهاز، ومن بعض المشاكل الّتي تسبّبت بها البرمجيّات الخبيثة من فيروساتvirus وديدان worms وغيرها نتيجة الاستخدام غير الآمن والمسؤول للشّبكة.
لذا قرّر أن يمنع استخدام الإنترنت في المختبر فتدخّلتم لإيجاد حلّ.
المجموعتان ١- ٢

الموضوع الثاني: الخداع والاحتيال على الإنترنت.

إنّ عددًا كبيرًا من الطّلاب يقعون في فخّ الخداع والاحتيال على الشّبكة، لذا قرّر أفراد المجموعتين الثّالثة والرّابعة أن يقوموا بحملة توعية عن هذا الموضوع.
المجموعتان ٣- ٤

مهمّة المجموعتين الأولى والثّانية:

عليكم أن تثبتوا لأستاذ/ة المعلوماتية بأنّكم أصبحتم تدركون مخاطر البرمجيّات الخبيثة الّتي تطول الحاسوب وبياناته، وتعرفون كيف تحمون أجهزة مختبر المعلوماتيّة منها أثناء استخدامكم الإنترنت، ثمّ تقدّمون عرضًا أمام الجميع في الصّفّ لتعريفهم إلى السّبيل الّذي يمكّنهم من تحمّل المسؤوليّة وحماية الحاسوب وبياناته من البرمجيّات الخبيثة. وبناء عليه من المحتمل أن يغيّر الأستاذ قراره.

توزيع أدوار ومهام أفراد المجموعة الأولى:

دور الفردين الأوّل والثّاني: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هي البرمجيّات الخبيثة malware ؟
٢- اذكرا أربعة أنواع من البرمجيّات الخبيثة.
٣- ما هو الفيروس التّقليدي والفيروس الماكرو؟
٤- كيف يصاب الحاسوب بالفيروس؟ وما هي بعض الأضرار الّتي يتسبّب بها؟
٥- اختارا فيروسًا معيّنًا، وأخبرا عن كيفيّة إصابة الجهاز به والأضرار الّتي يتسبّب بها.
٦- حدّدا كيفيّة حماية الحاسوب من الفيروسات وطريقة إزالتها عنه.

دور الفردين الثّالث والرّابع: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هي الدّيدان worms؟
٢- كيف يصاب الحاسوب بها؟ وما هي بعض الأضرار الّتي تتسبّب بها؟
٣- ما هي أحصنة طروادة Trojan Horses؟
٤- كيف يصاب الحاسوب بحصان طروادة Trojan horse ؟
٥- ما هي بعض الأضرار الّتي تتسبّب بها أحصنة طروادة؟
٦- كيف نحمي الحاسوب من أحصنة طروادة؟ وكيف نزيلها عنه؟

دور الفرد الخامس:

تصميم معلّقة، عن البرمجيّات الخبيثة على الإنترنت وتنفيذها، تحوي رسمًا توضيحيًّا من وحي الموضوع، ونصًّا يتمّ وضعه بالاتفاق مع باقي أفراد المجموعة، ولائحة بأهمّ القواعد الّتي تساعد على حماية الحاسوب من البرمجيّات الخبيثة، وتحترم حقوق الملكيّة الفكريّة والأدبيّة وحقوق النّسخ والنّشر. ثمّ يعرضها أمام جميع تلامذة الصّفّ، ويجيب عن الأسئلة المطروحة.

مهمّة المجموعتين الأولى والثّانية:

عليكم أن تثبتوا لأستاذ/ة المعلوماتية بأنّكم أصبحتم تدركون مخاطر البرمجيّات الخبيثة الّتي تطول الحاسوب وبياناته، وتعرفون كيف تحمون أجهزة مختبر المعلوماتيّة منها أثناء استخدامكم الإنترنت، ثمّ تقدّمون عرضًا أمام الجميع في الصّفّ لتعريفهم إلى السّبيل الّذي يمكّنهم من تحمّل المسؤوليّة وحماية الحاسوب وبياناته من البرمجيّات الخبيثة. وبناء عليه من المحتمل أن يغيّر الأستاذ/ة قراره.

توزيع أدوار ومهام أفراد المجموعة الثانية:

دور الفردين الأوّل والثّاني: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هو الـ Adware؟
٢- كيف يصاب الحاسوب بالـ Adware؟
٣- هل يتسبّب الـ Adware بالأضرار؟ إذا كان الجواب نعم فما هي؟
٤- ما هي برمجيّات التّجسّس spyware؟
٥- كيف يصاب الحاسوب ببرمجيّات التّجسّس spyware ؟
٦- هل تتسبّب برمجيّات التّجسّس الspyware بالأضرار؟ إذا كان الجواب نعم فما هي؟
٧- كيف نحمي الحاسوب من برمجيّات التّجسّس spyware؟

دور الفردين الثّالث والرّابع: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هو ال cookie؟
٢- كيف يصاب الحاسوب بالcookie ؟
٣- هل يتسبّب الcookie بالأضرار؟ إذا كان الجواب نعم فما هي؟
٤- ما هو البريد المزعج spam؟
٥- هل يتسبّب الspam بالأضرار؟ إذا كان الجواب نعم فما هي؟
٦- كيف نحمي البريد الإلكتروني من ال spam؟

دور الفرد الخامس:

تأليف أغنية (RAP) من وحي الموضوع تحوي أهمّ القواعد الّتي تساعد في حماية الحاسوب من البرمجيّات الخبيثة ثمّ يغنّيها أمام الصّفّ ويجيب عن الأسئلة المطروحة.

مهمّة المجموعتين الثّالثة والرّابعة:

على أفراد كلّ مجموعة أن يجمعوا المعلومات المطلوبة منهم، ثمّ يقدّموا عرضًا أمام زملائهم في الصّفّ ليعرّفوهم إلى أنواع الاحتيال والخداع على الشّبكة، وكيفيّة حماية البيانات الشّخصيّة من أجل تفادي الوقوع ضحيّة هذا العمل أثناء استخدام الإنترنت. ونتيجة هذا العرض سوف يتأكّد من في الصّفّ ما إذا كانوا قد أصبحوا قادرين على التّعرّف إلى أساليب الخداع والاحتيال الموجودة على الشّبكة، وكيفيّة تفادي الوقوع ضحيّتها أم لا.

توزيع أدوار ومهام أفراد المجموعة الثّالثة:

دور الفردين الأوّل والثّاني: إيجاد أجوبة عن الأسئلة الآتية:

١- سمّيا أربعة أساليب خداع واحتيال على الإنترنت.
٢- حدّدا من هم قراصنة الإنترنت hackers وماذا يفعلون؟
٣- لم تعتبر القرصنة فعلًا غير أخلاقي؟
٤- ما هو الphishing؟
٥- عدّدا بعضا من أساليب الphishing على الإنترنت.
٦- اشرحا كيف يمكن حماية المعلومات الشّخصيّة مثل الحساب وكلمة المرور من السّرقة؟

دور الفردين الثّالث والرّابع: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هو الscam؟ أعطيا أمثلة عنه.
٢- عدّدا بعض أضرار الscam.
٣- ما هو الفرق بين البريد الطّفيليspam و الscam.
٤- ما هو جدار النّار firewall؟ ما هي فوائده؟
٥- ما هو e-mail spoofing ؟ أعطيا أمثلة عنه.
٦- اذكرا بعض أضرار ال e-mail spoofing.

دور الفرد الخامس:

تصميم معلّقة، عن الخداع والاحتيال على الإنترنت وتنفيذها، تحوي رسمًا توضيحيًّا من وحي الموضوع، ونصًّا بأهمّ القواعد الّتي تساعد في الحماية من الخداع والاحتيال على الشّبكة، ثمّ عرضها أمام جميع تلامذة الصّفّ، والإجابة عن الأسئلة المطروحة.

مهمّة المجموعتين الثّالثة والرّابعة:

على أفراد كلّ مجموعة أن يجمعوا المعلومات المطلوبة منهم، ثمّ يقدّموا عرضًا أمام زملائهم في الصّفّ ليعرّفوهم إلى أنواع الاحتيال والخداع على الشّبكة، وكيفيّة حماية البيانات الشّخصيّة من أجل تفادي الوقوع ضحيّة هذا العمل أثناء استخدام الإنترنت. ونتيجة هذا العرض سوف يتأكّد من في الصّفّ ما إذا كانوا قد أصبحوا قادرين على التّعرّف إلى أساليب الخداع والاحتيال الموجودة على الشّبكة، وكيفيّة تفادي الوقوع ضحيّتها أم لا.

توزيع أدوار ومهام أفراد المجموعة الرابعة:

دور الفردين الأوّل والثّاني: إيجاد أجوبة عن الأسئلة الآتية:

١- سمّيا بعض أنواع إشاعات الإنترنت internet hoaxes؟ أعطيا أمثلة.
٢- عدّدا بعض الأضرار الّتي تتسبّب بها الإشاعات على الإنترنت.
٣- ما هو الchain e-mail؟ أعطيا أمثلة.
٤- ما هو ال internet frauds؟ أعطيا أمثلة.
٥- عدّدا بعض الأضرار الّتي يتسبّب بها ال internet frauds؟

دور الفردين الثّالث والرّابع: إيجاد أجوبة عن الأسئلة الآتية:

١- ما هي سرقة الهويّة Identity Theft ؟
٢- اذكرا بعضًا من أساليب سرقة الهويّة، وفسّرا نتائج ذلك على الضّحيّة؟
٣- ما هي الخطوات الّتي يجب اتخاذها في حال التّعرّض لسرقة الهويّة؟
٤- ما هو الفرق بين http و https؟
٥- اشرحا كيفيّة استخدام الwifi والbluetooth بشكل آمن.
٦- اذكرا القواعد الخاصّة باستعمال حاسوب أو هاتف غير شخصي، خصوصًا في مقاهي الإنترنت أو الأماكن العامّة؟

دور الفرد الخامس:

إيجاد أجوبة عن الأسئلة الآتية:

١- ما هي أهم القواعد لتفادي الخداع والاحتيال على الشّبكة؟
٢- اذكر أساليب عدّة لاختيار كلمة سرّ محصّنة.

بعد أن يقوم كلّ فرد بالمهام الموكلة إليه، على المجموعة تقديم عرض أمام جميع تلامذة الصّفّ والإجابة عن الأسئلة الّتي ستطرح.

التّطبيق (عمل فردي):

• قبل بدء عرض المجموعات لعملها، يطلب المعلّم/ة إلى كلّ تلميذ/ة ملء الجدول الآتي أثناء عرض المجموعات لعملهم.

ماذا أصبحت تعرف عن البرمجيّات الخبيثة؟	ماذا أصبحت تعرف عن الخداع والاحتيال على الشّبكة؟

النّشاط الثّاني (١٥ دقيقة):

• يوزّع المعلّم/ة عل كلّ مجموعة ورقة الكلمات المتقاطعة ويطلب إلى كلّ منها العمل على حلّها.
في حال توافرت أدوات لعرض الفيديو على المعلّم/ة أن يعرض النّشاط، ويقرأ النّقاط الموجودة في المطويّتين والّتي تطول الموضوع.
• حلّ الكلمات المتقاطعة:

V	I	R	U	S											
	D		S	P	O	O	F	I	N	G	E	M	A	I	L
	E			Y											
	N			W	O	R	M								
	T			A					C						
	I		T	R	O	J	A	N	H	O	R	S	E		
	T			E					A			C			
	Y								I			A			
	T								N			M			
	H								E						
	E						S	P	A	M					
	F									A	D	W	A	R	E
	T									I					
										L					

المعلومات

١. برنامج تجسّسي يتعقّب تحرّكاتك على الشّبكة العنكبوتيّة، ويعرف عنك معلومات كثيرة من دون علمك .
٢. برنامج خبيث يقوم بمضاعفة نفسه من خلال الإنترنت، وينتقل من جهاز إلى آخر، وهو يقوم باستخدام مصادر الكمبيوتر.
٣. برنامج خبيث يقوم بإدراج نفسه داخل ملفّ، ويهدف إلى تعطيل العمل في الكمبيوتر ولكنّه لا يستطيع مضاعفة نفسه.
٤. برنامج يعرض الإعلانات بصورة مستمرّة .
٥. برنامج خادع ويبدو كأنّه مفيد، ولكنّه بالحقيقة يهدّد أمن الكمبيوتر ويتسبّب بالأضرار.
٦. بريد إلكتروني يطلب إلى مستلمه أن يمرّره إلى عدّة أشخاص متذرّعا بالتّعاطف مع حالة إنسانية أو غيرها.
٧. بريد مزوّر يُرسل إليك عن طريق شخص لا تعرفه في الغالب، بحيث يظهر أنّ مرسل الرّسالة هو شخص ذو منصب معين (كمدير شركة أو بنك أو من فريق صيانة موقع معروف مثل facebook، hotmail، yahoo) ويطلب إلى المستخدم معلومات عن حسابه متذرّعًا بحجّة ما أو حالة طارئة فينخدع المستخدم بذلك ويستجيب لطلبه.
٨. بريد إلكتروني خادع يظهر وكأنّ مرسله هو شخص من قائمة اتصالاتك contact list.
٩. بريد إلكتروني مزعج، وغير مرغوب به، يُرسل إليكم بكمّ هائل.
١٠. جريمة معلوماتيّة يقوم بها الجناة عبر انتحال شخصيّة شخص ما، وذلك عن طريق سرقة معلوماته الشّخصيّة من دون علمه من أجل الحصول على مكسب مادي أو القيام بجريمة أخرى. وهذه الجريمة يعاقب عليها القانون.

صيتك حلو
offline و online؟*

* أنا ألتزم بالقواعد الأخلاقيّة على الإنترنت اذ ما يصحّ في حياتي الواقعيّة يصحّ في عالمي الرقمي أيضًا، لذا:

- أنا أُحافظ على سمعة رقمية جيّدة في خلال استخدامي الشبكة.
- أنا لن أقوم بنشر أيّ تعليقات أو صور مسيئة أو محرجة للآخرين.
- أنا لن أنضمّ إلى مجموعات مسيئة للآخرين أو مسيئة للمعتقدات والأديان والتي تُروّج لأفكار وقضايا تتنافى مع الأخلاق والآداب مثل العنصرية، التعصّب الديني او العرقي، العنف، الكراهيّة، الارهاب، التشجيع على تعاطي المخدرات والانتحار... وكذلك لن أُؤيّد هذه المجموعات.
- أنا لن أخرق قوانين الملكيّة الفكريّة ولن أنسخ موسيقىً وألعابًا وبرامجَ بصورة غير قانونيّة بل ألتزم بقواعد الآداب العامة المتعارف عليها اجتماعيًا.
- أنا أستشهد بالمصادر بالشّكل الصّحيح.
- أنا أُفكّر جيّدًا قبل أن أنشر أيّ محتوى على الإنترنت.



السّمعة الرقميّة والملكيّة الفكريّة

١- أتصرّف كما في الحياة الواقعيّة

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يحافظ على سمعة رقميّة جيّدة.

الموارد:
- يتعرّف، خلال عمله على الشّبكة، إلى سلوكيّات تنطبق عليها معايير الأخلاق وقواعد الآداب العامّة المتعارف عليها اجتماعيًّا.
- يتعرّف إلى ماهية قوانين الملكيّة الفكريّة وحقوق النّسخ والنّشر.

المعارف	المهارات والقدرات	المواقف
• ماهيّة العلاقة بين المجتمع والإنترنت. • ماهيّة حقوق الملكيّة الفكريّة.	• يطبق قواعد السّمعة الشّخصيّة على الإنترنت. • يعرف أنّ كل ما ينشر على الإنترنت يحفظ للأبد ولا يمحى.	• يرفض كتابة أو تدوين أيّة تعليق يسيء إلى أحد ما أو يجرح مشاعره. • يستشير شخصًا راشدًا يثق به قبل المشاركة بتأييد أي مجموعة، قبل تحميل أيّة صور شخصيّة وقبل استخدام أو نشر أيّ محتوى أو معلومات من أيّ مصدر. • يحترم خصوصيّة الآخر.

- **الفئة المعنيّة:** تلامذة الصّفّين الرّابع والخامس من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّتان كاملتان.
- **مستندات ووسائل الإيضاح:** فيديو السّمعة الرّقميّة – ورقة العمل ١ – كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٢٣-٢٤-٢٥.
- **نمط التنفيذ:** فردي ومجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز: (١٠ دقيقة)

- يشاهد التّلامذة الفيديو التّعليمي، ثمّ يقوم المعلّم/ة بسؤالهم عن رأيهم حول مضمونه، ويدير مناقشة لمدّة خمس دقائق.

- يرسم المعلّم/ة الجدول الآتي على اللّوح، ويكتب محتوى العمود الأوّل فقط، ثمّ يسأل التّلامذة: ما رأيكم بتصرّفات سامي؟

سامي على شبكة الإنترنت	سامي في المجتمع
أيّد سامي مجموعة «أغبى تلميذ في الصّفّ».	يحترم سامي رفاقه.
نشر سامي صورة محرجة لرفيقه على الإنترنت.	لا يجرح سامي مشاعر الآخرين.
شتم سامي رفيقه رامي لأنّه نشر على الإنترنت خبرًا مفاده أنّه يحبّ رانيا.	لا يشتم سامي أحدًا.

- بعد ذلك، يكتب المعلّم/ة محتوى العمود الثّاني من الجدول، ويسأل التّلامذة: ما رأيكم بتصرّفات سامي على شبكة الإنترنت؟ هل تغيّرت نظرتكم إلى سامي بعدما قرأتم تصرّفاته على شبكة الإنترنت؟
- يقود المعلّم/ة التّلامذة في هذه المناقشة إلى الاستنتاج الآتي: كما نتصرّف بأخلاقيّة في حياتنا الواقعيّة، نتصرّف بأخلاقيّة على شبكة الإنترنت أيضًا.

مرحلة التّعلّم: (٢٥ دقيقة)

- يجلب المعلّم/ة معه نسخًا عن الصّور الثلاثة الموجودة في ورقة العمل ١.

- يقسّم الصّفّ إلى ثلاث مجموعات، ويعطي كلّ مجموعة صورة. ثمّ يطلب إليهم كتابة تعليقاتهم عن الصّور كلّ بدوره (كما يفعلون على الشّبكات الاجتماعيّة).

- عند الانتهاء من كتابة التّعليقات يأخذ المعلّم/ة الصّور، ويقرأ بصوت عالٍ ما كتب عن كلّ منها.
- تبدأ المناقشة: ما رأيكم بهذه الصّورة؟ من كتب هذا التّعليق؟ ما رأيكم حول ما قيل؟..... لِمَ كتِب كذا وكذا تحت هذه الصّورة؟...... هل أستطيع أخذ جملة فلان واستخدامها كأنّني أنا من كتبها؟..... لِمَ تمّ التّعليق بطريقة سيئة عن هذه الصّورة وليس عن تلك؟ ما الفرق بين الصّورتين؟..... إذا رأيتم صورة لأحد أصدقائكم على هذا الشّكل ماذا تفعلون؟ إذا رأيتم صورة لأحد الأشخاص على هذا الشّكل وأنتم لا تحبّونه، فماذا تفعلون؟ ...... هل يجب أن نعلّق بشكل سيّء على أحد أيًّا كان؟ ....

التّطبيق (٢٠ دقيقة)

- يوزّع المعلّم/ة ورقة العمل ٢، ويطلب إلى التّلامذة العمل عليها بشكل فردي.

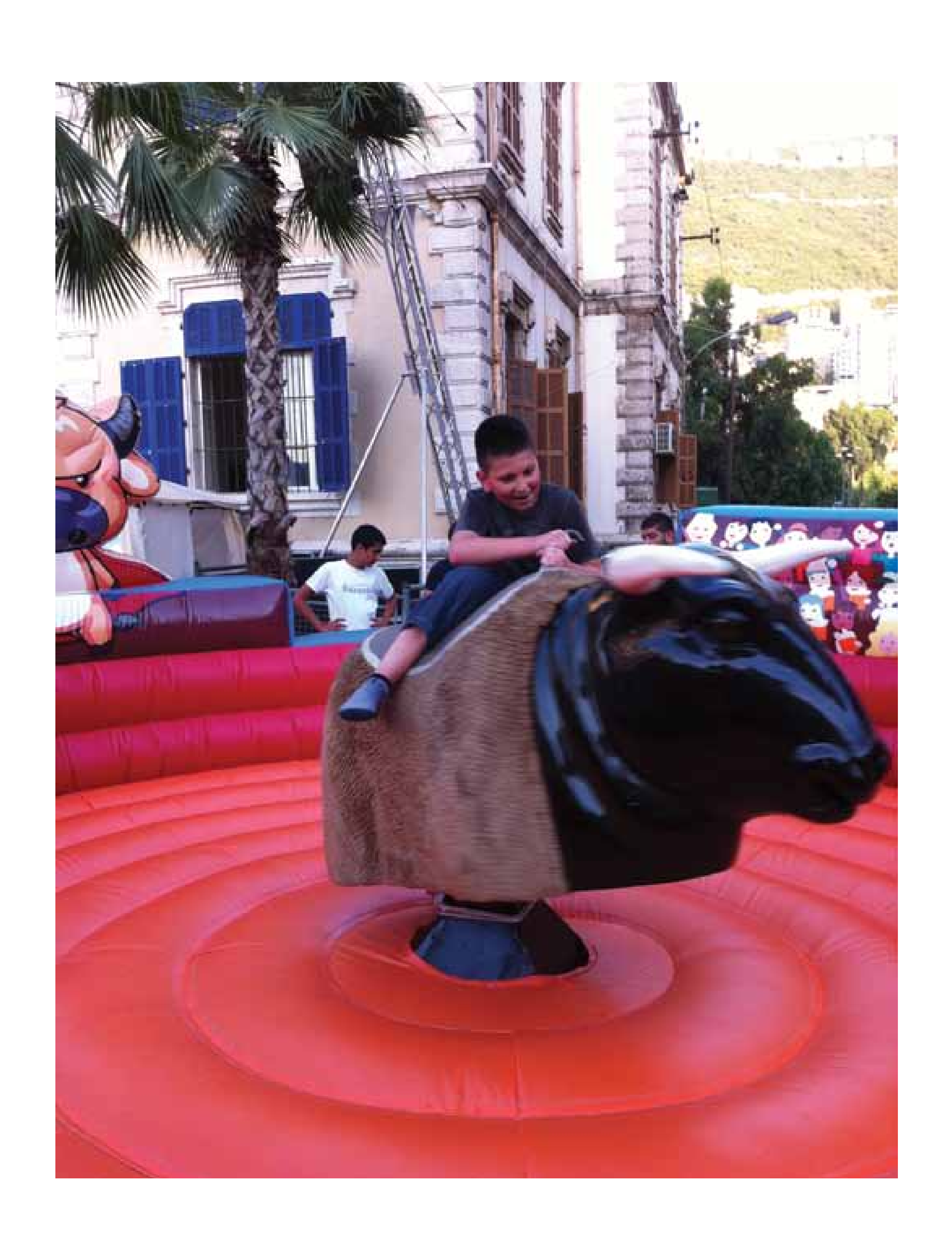
- عند الانتهاء، يقوم المعلّم/ة بمناقشة إجاباتهم ويشرح لهم النّقاط الآتية:

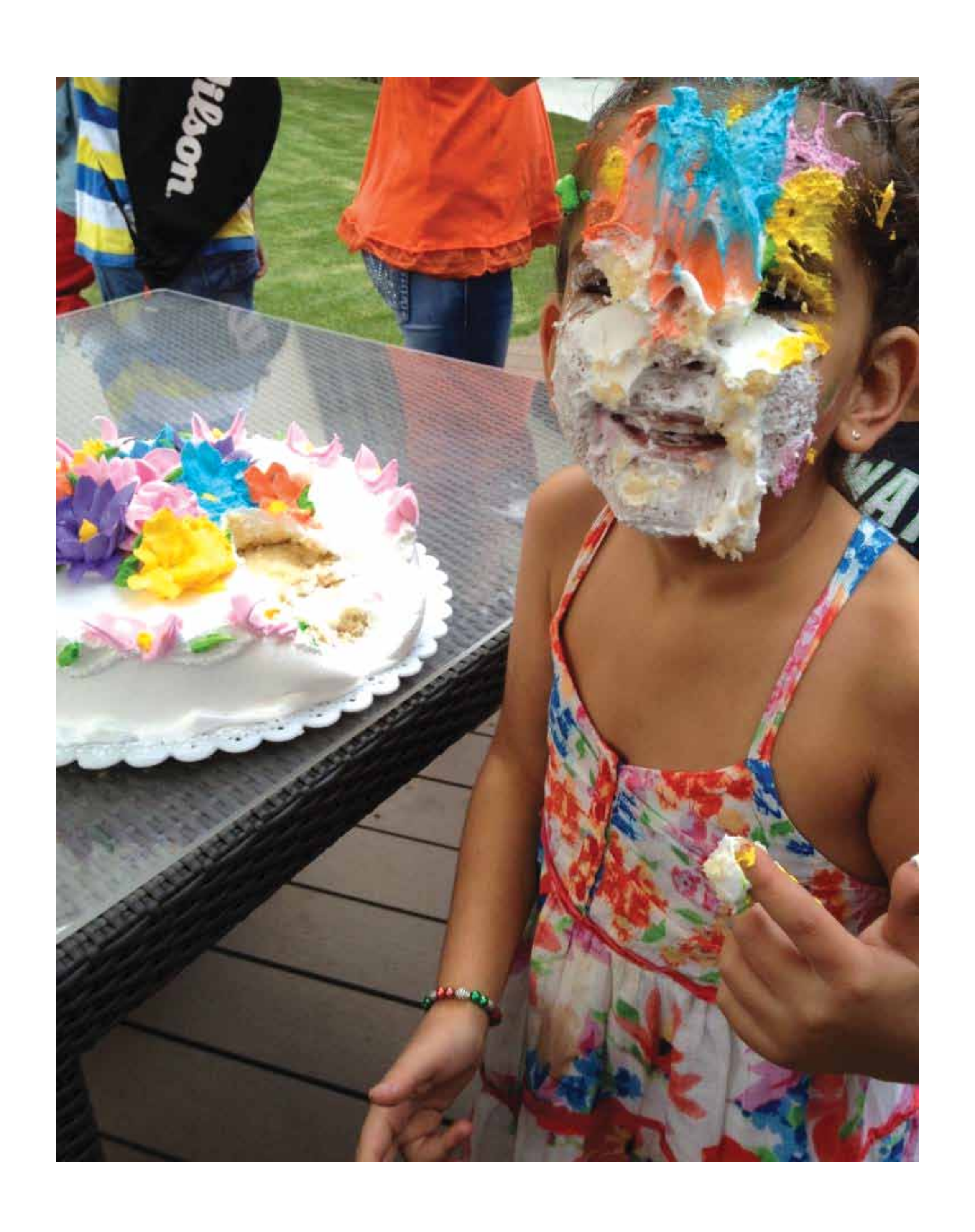
– لا يجب أن تزعج أصدقاءك بإرسال دعوات للعبة ما. وإذا قمت بإرسال الدّعوة إلى صديق ولم يقبلها فلا تزعجه بإرسالها مرّة أخرى. فكما لا تريد أن يقوم الآخرون بإزعاجك، لا تقم بإزعاجهم أنت أيضًا.
– عوضًا عن الشّجار وأذيّة الآخر، يجب إخبار شخص راشد (الأهل أو المعلّم/ة) لإيجاد الحل الأمثل. رغم أنّه من الصّعب الحفاظ على الهدوء عندما يسيء إلينا أحد، ولكنّ الرّدّ بالمثل هو أسوأ شيء يمكن أن تفعله، والتّجاهل لا يجعل الأشخاص يتوقّفون عن الإساءة إليك. فالحلّ الأفضل هو إخبار شخص راشد لكي يضع حدًّا لهم.
– عليك أنت أيضًا أن لا تسيء إلى الأشخاص أو تهينهم. تذكّر دائمًا « إفعل للآخرين ما تريد أن يفعله الآخرون لك».
– تذكر أيضًا أنّ كلّ من هم على الشّبكة يستطيعون قراءة ما تكتبه. وأنّ كلماتك مكتوبة ومحفوظة في مكان ما، ومن الممكن أن تعود لملاحقتك في يوم ما. يجب أن تكون حذرًا، فأنت لا تستطيع أن تتحكّم بمن قد تصل كلماتك إليهم.
– لا يريد أحد نشر صور محرجة له على الإنترنت. وإذا أردت نشر صورة (محرجة كانت أم لا) عليك أوّلا أخذ إذن كلّ من يظهر فيها. وإذا نشر أحدهم صورة محرجة لك من دون إذنك، لا تنفعل بطريقة مبالغة، كن هادئًا واطلب إليه إزالتها. وتذكر أنّ إزالة الأشياء عن الإنترنت لا يعني محوها نهائيًّا، فمن الممكن أن تكون ما زالت موجودة في مكان ما على الشّبكة، ومن الممكن أن يكون أحدهم قد نسخها وأرسلها إلى ملايين الأشخاص من دون علمك أو أخذ الإذن منك. لذلك فكّر جيّدا قبل أن تنشر أيّ شيء لأنّ ما تجده مضحكًا اليوم من الممكن أن يحرجك غدًا.
– قبل الانضمام إلى إحدى المجموعات على الشّبكة عليك أن تتأكّد من أنّها لا تسيء إلى الآخرين.
– كما أنّه من الأفضل استشارة شخص راشد قبل نشر أيّة صور كي تتأكد أنّه من الآمن نشرها ولا يمكن أن تسيء إليك أو إلى الآخرين.
– يمكن للتّلامذة استخدام الصّور أو النّصوص من الإنترنت في التّقارير والأبحاث المدرسيّة بشرط أن يعيدوا صياغة الجمل بطريقتهم الخاصّة، ويضعوا علامات اقتباس حول أيّة عبارة تستخدم كما هي، كما يجب ذكر المصدر أو الموقع الّذي أخذت هذه منه المعلومات.

- ومن أجل التّأكّد من صحّة المحتوى ومن إمكانية استخدامه، لا تستخدم أيّ محتوى أو معلومات من أيّ مصدر كان قبل استشارة شخص راشد تثق به.

ورقة عمل ١







ورقة عمل ٢

أضع علامة صحّ أمام التّصرّف الصّحيح.

وصف السّيناريو	كيفيّة التّصرّف
ذهب فادي إلى بيتك ليلعب معك. دقّ الباب ولم يجب أحد. ماذا يفعل؟	☐ يدقّ الباب مرارًا وتكرارًا وبقوّة أكبر. ☐ يدقّ الباب مرّة أخرى وإذا لم يجب أحد، يعود إلى بيته. ☐ لا يدقّ مرة أخرى ويعود إلى بيته.
أرسل فادي لك دعوة للانضمام إلى أحد الألعاب على الإنترنت. لم تلبِّ الدعوة. فماذا يفعل؟	☐ يعيد إرسال الدّعوة مرّات عديدة لدرجة أنّك ستقبلها فقط كي تستريح من الإزعاج. ☐ يعيد إرسال الدّعوة مرّة أخرى فقط. ☐ لايعيد إرسال الدّعوة كي لا يزعجك.
شتمك ربيع في المدرسة. ماذا تفعل؟	☐ تشتمه في المقابل وتتعاركا. ☐ لا تردّ عليه ولا تعره اهتمامًا. ☐ لا تجيبه وتخبر المعلّم/ة.
كتب ربيع شيئًا مسيئًا عنك على الإنترنت. ماذا تفعل؟	☐ تكتب عنه شيئًا مسيئًا أنت أيضًا. ☐ لا تردّ عليه، ولا تعره اهتمامًا. ☐ تخبر شخصًا راشدًا كي يتصرّف.
رأت سلوى دفتر يوميّاتك مفتوحًا على الطّاولة. ماذا تفعل؟	☐ تقرأ بعض محتوياته. ☐ تأخذه وتعيده إليك حتّى لا يراه أحد آخر. ☐ لا تهتمّ بالأمر.
وجدت سلوى أنّك قد تركت بريدك الالإلكتروني مفتوحًا. ماذا تفعل؟	☐ تقرأ بعض محتوياته. ☐ تغلقه لك حتّى لايأتي أحد آخر ويقرأ ما فيه. ☐ لا تهتمّ بالأمر وتتركه كما هو.

دعاك فادي لتلعب معه ومع مجموعة أصدقائه الجدد. سألت أمّك فطلبت إليك الابتعاد عنهم لأنّهم لا يحسنون التّصرّف. ماذا تفعل؟	☐ لا تهتمّ بكلام أمّك. ☐ تلعب معهم من دون أن تشاركهم في التّصرّفات السّيّئة. ☐ تسمع كلام أمّك وتبتعد عنهم.
أرسل إليك فادي دعوة للانضمام الى مجموعة على الإنترنت. ماذا تفعل؟	☐ تنضمّ إليها لأنّ رفيقك قد انضم إليها. ☐ تتأكّد من مواضيع المجموعة لتتأكّد أنّها تثير اهتمامك. ☐ تستشير شخصًا راشدًا لتتأكّد من أنّها لا تسيء للآخرين.
قامت عائلتك وعائلة رامي برحلة معا. أراد رامي أن ينشر صور الرّحلة على الإنترنت. ماذا يفعل؟	☐ ينشر كلّ الصّور حتّى المحرجة منها. ☐ يتأكّد أنّ لا مشكلة لديك في نشر أيّة صورة. ☐ يطلب مساعدة شخص راشد في وضع الصّور المحرجة جانبًا حتّى لا ينشرها.
عرضت عليك سمر المساعدة عن طريق السّماح لك بنسخ بحثها المدرسي. ماذا تفعل؟	☐ تنسخ قطعا من بحثها. ☐ تقرأ بحثها لتأخذ أفكارا ثمّ تكتب البحث بطريقتك الخاصّة. ☐ تسأل شخصًا راشدًا إذا كان يسمح لك نسخ عمل شخص آخر.
وجدت على الإنترنت، نصًّا مناسبًا تمامًا لموضوع بحثك، ففكّرت أن تنسخه كما هو. ماذا تفعل؟	☐ تنسخ النّصّ وتقدّمه للمعلّمة. ☐ تقرأ النّصّ لتأخذ أفكارًا ثمّ تكتب البحث بطريقتك الخاصّة. ☐ تسأل شخصًا راشدًا إذا كان يسمح لك نسخ البحث عن الإنترنت.

٢- ما هو التّصرف الصّحيح؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يحافظ على سمعة رقميّة جيّدة.

الموارد:
- يستخدم، خلال عمله على الشّبكة، سلوكيّات تنطبق عليها معايير الأخلاق وقواعد الآداب العامّة المتعارف عليها اجتماعيًّا.

المعارف	المهارات والقدرات	المواقف
• ماهيّة العلاقة بين المجتمع والإنترنت.	• يطبّق قواعد السّمعة الشّخصيّة على الإنترنت. • يدرك أنّ لكلّ مستخدم نوع من الأثر الرّقمي. • يفهم أنّ ما ينشر على الإنترنت يحفظ للأبد ولا يمحى	• يرفض الإساءة إلى الآخرين أو للمعتقدات والأديان. • يحترم خصوصيّته وخصوصيّة الآخر.

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** فيديو السّمعة الرّقميّة – ورقة عمل ١– مستند رقم ١ – ورقة عمل ٢ ، كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٢٣-٢٤-٢٥
- **نمط التّنفيذ:** فردي ومجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق):

- يشاهد التّلامذة الفيديو التّعليمي، ثمّ يقوم المعلّم/ة بسؤالهم عن رأيهم بمضمونه، ويدير مناقشة لمدّة خمس دقائق.

- أو يعرض المعلّم/ة المستند رقم ١ ثم يطرح السؤال الآتي: ما الصّلة بين تصرّفاتنا في الحياة الواقعيّة وعلى الشّبكة؟ ويدير نقاشًا حول واقع حياتهم المعيش والواقع كما هو على صفحات الإنترنت ومواقع التّواصل الاجتماعي... فكما لا ننشر صورنا على الطّريق العامّ، كذلك لا ننشر صورنا على صفحاتنا في مواقع التّواصل الاجتماعي. وكما نحافظ على سمعتنا الشّخصيّة في المجتمع يجب أن نحافظ عليها على الإنترنت.

- يستنتج التّلامذة في النّهاية الإجابة عن السّؤال الّذي طرحه المعلّم/ة: نعتمد المعايير الأخلاقيّة نفسها في تصرّفاتنا سواء أكان ذلك في حياتنا الواقعية أم على صفحات الإنترنت ومواقع التّواصل الاجتماعي.

مرحلة التّعلّم: (٢٥ دقيقة)

- يطلب المعلّم/ة إلى التّلامذة العمل ثنائيّا على حلّ ورقة العمل ١. وعند الانتهاء، يصار إلى مناقشة الإجابات جماعيًّا مع التّركيز على هدف كل سؤال:

١) لا يجب أن تزعج أصدقاءك بإرسال دعوات للعبة ما. وإذا قمت بإرسال الدّعوة إلى صديق ولم يقبلها فلا تزعجه بإرسالها مرّة أخرى. فكما لا تريد أن يقوم الآخرون بإزعاجك، لا تقم أنت بإزعاجهم أنت أيضًا.

٢) عوضًا عن الشّجار وأذيّة الآخر، يجب إخبار شخص راشد (الأهل أو المعلّم/ة) لإيجاد الحل الأمثل. رغم أنّه من الصّعب الحفاظ على الهدوء عندما يسيء إلينا أحد، ولكنّ الرّدّ بالمثل هو أسوأ شيء يمكن أن تفعله، والتّجاهل لا يجعل الأشخاص يتوقّفون عن الإساءة إليك. فالحلّ الأفضل هو إخبار شخص راشد لكي يضع حدًّا لهم.

- عليك أنت أيضًا أن لا تسيء إلى الأشخاص أو تهينهم. تذكّر دائمًا «إفعل للآخرين ما تريد أن يفعله الآخرون لك».

- تذكّر أيضًا أنّ كلّ من هم على الشّبكة يستطيعون قراءة ما تكتبه. وأنّ كلماتك مكتوبة ومحفوظة في مكان ما، ومن الممكن أن تعود لملاحقتك في يوم ما. يجب أن تكون حذرا، فأنت لا تستطيع أن تتحكّم بمن قد تصل كلماتك إليهم.

- قبل الانضمام إلى إحدى المجموعات على الشّبكة عليك أن تتأكّد من أنّها لا تسيء إلى الآخرين.

- لا يريد أحد نشر صور محرجة له على الإنترنت. وإذا أردت نشر صورة (محرجة كانت أم لا) عليك أوّلا أخذ إذن كلّ من يظهر فيها. وإذا نشر أحدهم صورة محرجة لك من دون إذنك، لا تنفعل بطريقة مبالغة، كن هادئًا واطلب إليه إزالتها. وتذكّر أنّ إزالة الأشياء عن الإنترنت لا يعني محوها نهائيًا، فمن الممكن أن تكون ما زالت موجودة في مكان ما على الشّبكة، ومن الممكن أن يكون أحدهم قد نسخها وأرسلها إلى ملايين الأشخاص من دون علمك أو أخذ الإذن منك. لذلك فكّر جيّدًا قبل أن تنشر أيّ شيء لأنّ ما تجده مضحكًا اليوم من الممكن أن يحرجك غدا.

- تذكّر دائمًا بأنّه ليست لديك أيّة خصوصيّة على الإنترنت. فخصوصيّتك يمكن أن ينتهكها الآخرون كما أنّ خصوصيّة الآخرين تعتمد عليك.

التّطبيق(١٠ دقائق)

- يوزّع المعلّم/ة نسخًا عن ورقة العمل ٢ ويطلب إلى التّلامذة العمل عليها بشكل فرديّ، ليصار بعد ذلك إلى مناقشتها بشكل جماعي.

ورقة عمل ١

- يحوي كلّ قسم أدناه قصّتين. أقترح نهاية جيّدة للقصّة الأولى وأخرى سيّئة. وأكرّر العمليّة نفسها مع القصّة الثّانية بعد مقارنتها بالأولى .

١) ذهب فادي إلى بيت صديقه سامي ليلعب معه.
دقّ الباب ولم يجب أحد.

دقّ الباب بقوّة مرارًا وتكرارًا، فخرج والد سامي وأنّبه لأنّه أيقظه.
....

لم يعاود دقّ الباب مرّة أخرى، وعاد إلى بيته.
....

أرسل فادي لسامي دعوة للانضمام إلى أحد الألعاب على الإنترنت
رفض سامي الدّعوة.

....
....

....
....

٢) شتم ربيع داني في المدرسة.

....
....

....
....

كتب ربيع شيئًا مسيئًا عن داني على الإنترنت.

....
....

....
....

٣) رأت سلوى دفتر يوميّات أختها ندى على الطّاولة.

....
....

....
....

وجدت سلوى أنّ أختها ندى قد تركت بريدها الإلكتروني مفتوحًا.

....
....

....
....

٤) دعا فادي صديقه ناجي ليلعب معه ومع مجموعة أصدقائه الجدد.

....	....
....	....

أرسل فادي دعوة إلى ناجي للانضمام إلى مجموعة على الإنترنت.

....
....

٥) عاد وليد ورامي من رحلة قامت بها عائلتاهما معًا. أراد وليد أن يطلع أصدقاءهما في المدرسة على صور الرّحلة.

....	....
....	....

أراد وليد نشر صور الرّحلة على الإنترنت.

....	....
....	....

ورقة عمل ٢

- أضع علامة صح أمام الجمل الصّحيحة، وأصحّح الخطأ في الجمل الباقية.

☐ الإنترنت كالمجتمع، ولكلّ شخص مسؤوليّات وواجبات تجاه الآخرين.

☐ على الإنترنت ليس لديّ مسؤوليّات وواجبات تجاه الآخرين.

☐ إذا قام أحد بإزعاجي أكتب تعليقًا مسيئًا عنه على الإنترنت.

☐ أؤيد أيّة مجموعة قام أحد أصدقائي بتأييدها.

☐ أنا أتمتع بالحرّيّة لذا أكتب أي شيء أريده على الإنترنت.

☐ إذا ذهبت برحلة مع أصدقائي أنشر كلّ الصّور الّتي التقطّها على الإنترنت.

☐ أطلب إذن الشّخص قبل تحميل صور له.

☐ أحمّل صوري الشّخصيّة على الإنترنت بغض النّظر عمّا أرتديه فيها.

☐ يمكنني أن أقوم بإلغاء ما نشرته ساعة أشاء من دون أن يبقى له أثر.

☐ إنّ كلّ ما ينشر على الإنترنت يحفظ للأبد ولا يمحى أبدًا.

٣- هل أنا مواطن رقمي صالح؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي ، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يحافظ على سمعة رقميّة جيّدة.

الموارد:

- يستخدم خلال عمله على الشّبكة، سلوكيّات تنطبق عليها معايير الأخلاق وقواعد الآداب العامّة المتعارف عليها اجتماعيًّا.

المعارف	المهارات والقدرات	المواقف
• ماهيّة العلاقة بين المجتمع والإنترنت.	• يطبّق قواعد السّمعة الشّخصيّة على الإنترنت. • يعرف أنّ كل ما ينشر على الإنترنت يحفظ للأبد ولا يمحى. • يدرك أنّ لكلّ مستخدم نوع من الأثر الرّقمي.	• يرفض الإساءة إلى الآخرين أو للمعتقدات والأديان. • يحترم خصوصيّته وخصوصيّة الآخر.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** نسخة عن أكثر الـemoticons استعمالاً وما تمثّله من معنى، ونسخة عن الاختصارات الأكثر استعمالاً – مستند رقم ١ – اختبار «هل أنا مواطن رقمي صالح» – وثيقة عمل ١ و ٢، كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ٢٣-٢٤-٢٥
- **نمط التّنفيذ:** فردي ومجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التحفيز (١٠ دقائق):

- يكتب المعلّم/ة على ورقة كبيرة «كيف أحافظ على سمعتي الشّخصيّة؟» ويطلب إلى التّلامذة أن يفكّروا لمدّة ثلاث دقائق، ثمّ يكتب كلّ منهم على ورقة أمامهم الجواب الّذي يراه مناسبًا. بعد ذلك يقرأ كلّ بدوره ما كتبه. وتتمّ مناقشة الجمل غير الواضحة، وأخيرًا يعلّقها المعلّم/ة على الورقة الكبيرة.
- عند إنهاء النّشاط يعرض المعلّم/ة المستند رقم ١ ثم يسأل: « برأيكم هل ما نفعله أو ننشره على الإنترنت يؤثّر في سمعتنا الشّخصيّة؟»

مرحلة التّعلّم: (٣٠ دقيقة):

- يوزِّع المعلّم/ة على التلامذة نسخًا عن اختبار «هل أنا مواطن رقمي صالح؟ – وثيقة عمل ١» ويطلب إليهم حلّه بشكل فرديّ.
- عند إنهاء النّشاط يتناقش المعلّم/ة وتلامذته بمضمون الأسئلة جميعها.

التّطبيق(١٠ دقائق)

- يطلب المعلّم/ة إلى كلّ مجموعة من ٤ أشخاص كتابة تعريف للسّمعة الرّقميّة. وبعد مناقشة الإجابات يعلّق أحدهم التّعريف الأفضل على اللّوح.
- في نهاية الحصّة، يقوم المعلّم بتوزيع نسخة عن أكثر الـemoticons استعمالاً والمعاني التّي تمثّلها، ونسخة عن الاختصارات الأكثر استعمالاً (مستند ١).

ملاحظة :
إذا تبقّى بعض الوقت، ينفّذ التّلامذة التّمرين الموجود في وثيقة عمل ٢ بشكل فردي، وذلك قبل أن يوزّع لهم النّسخ عن الـemoticons والاختصارات الأكثر استعمالاً.
أو يقسّم المعلّم الصف إلى مجموعات عمل، ويطلب إلى كلّ مجموعة كتابة الـ emoticons والـ acronyms التّي يستخدمونها على الإنترنت بالإضافة إلى معانيها.
تناقش الإجابات جماعيًّا على اللّوح ويتمّ توحيدها في جدول.
وينهي المعلّم/ة النّشاط بطرح السؤال الآتي ومناقشته مع التلامذة : «ماذا يحصل لو أرسلنا emoticons إلى شخص ما وفسّرها بطريقة غير صحيحة؟»

مستند رقم ١



وثيقة عمل ١

اختبار
«هل أنا مواطن رقمي صالح؟»

أختار جوابًا واحدًا لكلّ سؤال من الأسئلة الآتية:

١-خلال نقاش على الشّبكة، سألك أحد الأصدقاء سؤالًا تقنيًا سهلًا جدًّا، ويفترض على الجميع معرفته. ما هو الجواب الأمثل الّذي يجب أن تكتبه:

أ) «ما هذا السّؤال السّخيف، كيف لك أن تسأله؟»
ب) «غير معقول، لا يوجد أحد لا يعرفه؟»
ج) «فتّش أنت، واكتشف بنفسك الإجابة»
د) «أنا أعرف الإجابة، سوف أكتب لك ما ستفعله»

٢-كتب أحدهم شيئًا مسيئًا إليك. ماذا تفعل؟

أ) تكتب شيئًا مسيئًا أنت أيضًا.
ب) ترسل إليه email تشتمه فيه.
ج) لا تفعل شيئًا، ولا تهتمّ بما كتبه.
د) تخبر شخصًا راشدًا لكي يتصرّف.

٣-أنت غاضب جدا من أحد زملائك في الصّفّ فقررت أن تكتب عنه شيئا مسيئًا إليه لكي تنتقم منه. ماذا تفعل؟

أ) تكتب شيئًا مسيئًا إليه، ولكنّك تستخدم اسمًا مستعارًا.
ب) تكتب عنه شيئًا مسيئًا إليه، ولكنّك تستخدم اسمك الحقيقي وليس اسمًا مستعارًا.
ج) تكتب ما تريد، فأنت لديك حرّيّة الرّأي والتّعبير وبإمكانك قول أيّ شيء تريده.
د) لا تكتب شيئًا، فهذه ليست طريقة جيّدة لحلّ المشاكل بل إنّها إساءة وقد تندم عليها لاحقًا.

٤-قرأت ملاحظة مسيئة إلى أحد زملائك في الصّفّ وأنت لا تحبّه. ماذا تفعل؟

أ) تنضمّ إلى النّقاش، وتكتب تعليقات مسيئة إليه أنت أيضًا.
٢) لا تنضم إلى النّقاش، ولكن تفتح الصّفحة من وقت لآخر للاستمتاع بقراءة التّعليقات المسيئة.
ج) تتجاهل هذه التّعليقات والنّقاشات.
د) تخبر شخصًا راشدًا.

٥- أنت في حفلة مع أصدقائك، وكنتم تتصرّفون بعفويّة، وتمازحون بعضكم بعضًا. وأُخِذَت صورة لك مع عدد من أصدقائك ووجوهكم عليها كريما قالب الحلوى. ماذا تفعل؟
أ) تضع الصّورة على الإنترنت مع اسم كلّ من فيها لكي يتمكّن جميع من في المدرسة من رؤيتها.
ب) تضع الصّورة على الإنترنت مع عدم ذكر الأسماء.
ج) تضع الصّورة على الإنترنت بعد أخذ إذن من كلّ من فيها.
د) لا تضع الصّورة أبدًا على الإنترنت.

٦- نشر صديقك صورة محرجة لك من دون إذنك وطلبت إليه إزالتها. فاعتذر منك على هذا الخطأ ووعدك بأن يزيلها. وبعد **فترة، أرسل لك أحدهم الصّورة نفسها. فماذا تفعل؟**
أ) تتّصل بصديقك وتشتمه لأنّه لم يزلها.
ب) تشكّ بأنّ صديقك قد تركها ليهزأ بك.
ج) تغضب من صديقك لأنّه لم يفِ بوعده.
د) لا تغضب من صديقك فلا ذنب له إذا أخذ أحدهم الصّورة من صفحته من دون إذنه قبل أن يحذفها، وتطلب إليه ألّا يضع أيّة صورة تخصّك قبل استشارتك.

٧- كنت تلعب لعبةً جماعيّة على الإنترنت. وكلّما قمت بإدخال لاعب جديد تربح نقاطا كثيرة. ماذا تفعل؟
أ) تقوم بإرسال الدّعوات إلى جميع أصدقائك مرّات عديدة لدرجة أنّهم سيقبلونها فقط كي يستريحوا من الإزعاج.
ب) تقوم بدعوة كلّ أصدقائك إلى اللّعبة، ومن يقبل الانضمام إليك فيها يكسبك نقاطا جديدة.
ج) تقوم فقط بدعوة الأصدقاء الّذين تعرف أنّه قد تهمّهم اللّعبة أو الّذين قد أرسلوا إليك سابقا دعوة وقبلتها.
د) لا تقم بدعوة أحد أبدًا لأنّك لا تريد إزعاجهم.

٨- عند الانضمام إلى إحدى المجموعات على الشّبكة، عليك أن:
أ) تطرح كلّ ما تريد من مواضيع بغضّ النّظر عن التّوجّه الأساسي للصّفحة.
ب) تبحث عن الأسئلة الأكثر تداولًا كي لا تعيد طرحها.
ج) تقرأ بعض المواضيع المطروحة لأخذ فكرة عن الجوّ العامّ للمجموعة كي لا تكتب شيئًا لا يثير اهتمام المنتسبين إليها.
د) تقرأ المواضيع والتّعليقات في الصّفحة قبل الانضمام إليها للتّأكّد من أنّ هذه المجموعة لا تسيء إلى أحد.

٩- طرحت موضوعًا في مجموعة انضممت إليها. أجابك أحدهم بطريقة قاسية. ماذا تفعل؟
أ) تشتمه بأقبح الشّتائم.
ب) ترسل فيروسًا إلى عنوانه البريدي.
ج) تكتب إلى المسؤول عن الصّفحة تطلب إليه إلغاء عضويّته.
د) تكتب إليه بطريقة مهذّبة أن يكون لائقًا على الشّبكة.

١٠- جلست أمام جهاز كمبيوتر في أحد المقاهي، ووجدت أنّ من كان يجلس قبلك قد نسي بريده الإلكتروني مفتوحًا ماذا تفعل؟

أ) تقوم بسرقة بريده الإلكتروني، فهذا الغبي هو من ترك الفرصة سانحة.
ب) تنتظر قليلًا لاحتمال أن يتذكّر ويعود لإقفال حسابه، ثمّ تفعل ما تريد.
ج) تنظر إلى محتوياته من باب الفضول فقط ثمّ تقفله.
د) تقفله من دون النّظر إلى محتوياته.

١١- ما الّذي يمكنك كتابته في غرفة الدّردشة chat room؟

أ) كلّ ما تريده لأنّ الشّخص الّذي تتحدّث إليه يستطيع قراءة ما تكتبه فقط.
ب) كلّ ما تريده لأنّ الشّخص الّذي تتّحدث إليه والّذي يجلس بجانبك يستطيعان قراءة ما تكتبه فقط.
ج) كلّ ما تريده بشرط أن لا يكون شخصيًّا أو مسيئًا إلى أحد، لأنّ كلّ من هو داخل غرفة الدّردشة يستطيع قراءة ما تكتبه.
د) كلّ ما تريده بشرط أن لا يكون شخصيًّا أو مسيئًا إلى أحد لأنّ كلّ من هو على الشّبكة يستطيع قراءة ما تكتبه إذا أراد.

١٢- أنت تستخدم ، كما الجميع، الاختصارات للكتابة والتّواصل بطريقة سريعة وسهلة. مثلا BRB تعني be right back أيّ أعود بعد قليل. و 2moro تعني tomorrow أيّ غدًا. برأيك ماذا تعني 10Q :

أ) ليس لها أيّ معنى، هذا الاختصار غير متعارف عليه.
ب) ten quotes عشرة أمثلة (أقوال).
ج) Thanks
د) Thank You

١٣- أنت تستخدم، كما الجميع، الرّموز لتعبيرات الوجه Emoticons ، لتعبّر عن شعورك. مثلاً (: تعني الابتسامة أو السّعادة.

برأيك ماذا تعني :V-
أ) الضّحك.
ب) التّعجب.
ج) الصّراخ.
د) التّكلّم بصوت عال.

١٤- أرسل إليك صديقك رسالة email ووجدتها مضحكة جدًّا، وليس فيها أيّ شيء شخصيّ. قرّرت أن ترسلها إلى بقيّة أصدقائك، فما هي الطّريقة الأمثل لفعل ذلك؟

١) تعيد إرسالها إلى الجميع كما هي forward.

٢) تضع محتواها على صفحتك لكي يستطيع الجميع قراءتها.

ج) تعيد إرسالها إلى جميع أصدقائك مع الانتباه إلى محو عنوان email address الصّديق الّذي أرسلها أوّلاً.

د) تعيد إرسالها بعد سؤال صديقك الّذي أرسلها لك.

١٥- أرسل إليك صديقك رسالة email.

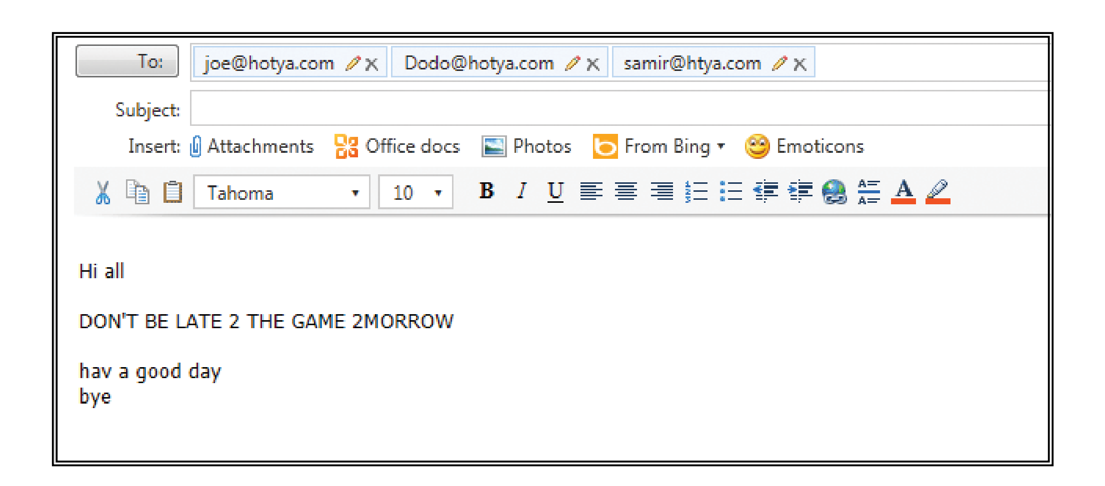
ما الخطأ الّذي ارتكبه؟

أ) لم يكتب عنوانًا للرّسالة.

ب) كتب بالأحرف الكبيرة capital letters.

ج) وضع كلّ العناوين في ال to.

د) كلّ ما سبق.



أعدُّ النّقاط لأعرف ما إذا كنت مواطنًا رقميًّا صالحًا.

الجواب أ : نقطة واحدة.
الجواب ب : نقطتان.
الجواب ج : ثلاث نقاط.
الجواب د : أربع نقاط.

إذا كان مجموع نقاطك أقل من ٢٥ :

أنت تقوم بنشر كلّ ما تفكّر فيه، وكلّ ما يصل إلى يدك حتّى لو كان شخصيًّا أو مسيئًا إلى الغير. حياتك الخاصّة ليست فعليًّا خاصّة. فكلّ ما يتعلّق بك أو بمحيطك منشور على الإنترنت.

انتبه، هذا النّوع من التّصرّفات يجلب لك الكثير من الأعداء. يجب أن لا تسيء إلى الأشخاص أو تهينهم، ولا تزعج الآخرين بهدف التّسلية. فكّر بما ستشعر به لو أنّ أحدهم فعل بك الشّيء نفسه؟

إذا كان مجموع نقاطك بين ٢٥ و ٤٠ :

أنت تقوم بنشر كلّ ما تفكّر فيه، وكلّ ما يصل إلى يدك حتّى لو كان شخصيًّا أو مسيئًا إلى الغير. أنت تزعج الأشخاص الّذين لا تستلطفهم، ولا تتوانى عن أذيّة من يسيء إليك ولو من دون قصد.

أنت تكتب ما يخطر ببالك، ولا يهمّك إذا فهمك الآخرون بطريقة خاطئة.

انتبه، هذا النّوع من التّصرّفات يجعلك عرضة للتّنمّر والأذيّة من الآخرين.

حاول أن تكون شخصًا أفضل. فإذا أساء إليك أحدهم لا تبادله الإساءة نفسها. وكن حذرًا في ما تنشره.

وحاول أن تكون لطيفًا مع الأشخاص وبذلك لن يكون لديهم سبب كي لا يكونوا لطفاء معك.

إذا كان مجموع نقاطك بين ٤٠ و ٥٥ :

أنت تحاول القيام بالتّصرّف الصّحيح. أنت لا تنشر كلّ ما يخطر ببالك، أو كل ما تلتقط من صور على الإنترنت بل تحاول أحيانًا كثيرة اختيار ما هو غير محرج وغير شخصي لتنشره. لكن غالبًا ما يكون اختيارك خاطئًا.

ما تكتبه أو تنشره يُفهم خاطئًا بشكل خاطئ ما يسبّب لك المشاكل. عندما يسيء إليك أحد فأنت، أحيانا، تردّ بالمثل وأحيانا أخرى تتجاهل الموضوع. وهذان الخياران خاطئان، فالرّدّ بالمثل هو أسوأ شيء يمكن أن تفعله، والتّجاهل لا يجعل الأشخاص يتوقّفون عن الإساءة إليك. فالحلّ الأفضل هو إخبار شخص راشد لكي يضع حدًّا لهم.

وبناء على ما تقدّم، وللاستمتاع بالإنترنت بطريقة آمنة عليك أن تحترم آراء الآخرين، وأن تكون حذرًا وواضحًا بما تكتبه أو تنشره. وتذكّر دائمًا « إفعل للآخرين ما تريد أن يفعله الآخرون لك».

إذا كان مجموع نقاطك أكثر من ٥٥ :

أنت شخص ذكيّ، وحسّاس، وتحترم آراء الآخرين وخصوصيّاتهم. أنت تفكّر دائمًا بشعور الآخر قبل أن تنشر أيّ شيء. أنت تقرأ ما تكتبه مرّات عدّة قبل نشره كي تتأكّد من وضوحه، وأنّ معناه لن يُفْهَمَ بشكل خاطئ. أنت شخص حذر أيضًا تحبّ أن تُبْقي كلّ ما يتعلّق بحياتك الشّخصيّة خاصًّا وسرّيًّا. كما أنّه لا مشكلة لديك بطلب المساعدة من شخص راشد عندما تجد حاجة لذلك. أنت لا تحبّ المتنمّرين وتحاول أن لايكون لك علاقة بأيّ منهم. أنت باختصار مواطن رقمي صالح.

شرح كلّ سؤال:

١- عليك أن تكون صبورًا، وأن تساعد الآخرين، وفكّر أنّه ليس لدى كلّ شخص الخبرة والمعرفة نفسها. والإنترنت هو كالمجتمع، ولديك مسؤوليّات وواجبات تجاه الآخرين المشتركين فيه. وكذلك إفعل للآخرين ما تريد أن يفعله الآخرون لك. وإذا أردت أن تسأل عن أيّ شيء انتبه إلى استخدام الأسلوب الصّحيح: لا تستخدم أسلوبًا وقحًا أو تضيّع وقت النّاس وإلّا فلن يرغب أحد بمساعدتك. وعند طرح سؤال، اشرح المشكلة باختصار، واسأل السّؤال بوضوح.

٢- أيضًا عن الشّجار وأذيّة الآخر، يجب إخبار شخص راشد (الأهل أو المعلّم/ة) ليجد الحلّ الأمثل. رغم أنّه من الصّعب الحفاظ على الهدوء عندما يسيء إلينا أحد، ولكنّ الرّدّ بالمثل هو أسوأ شيء يمكن أن تفعله، والتّجاهل لا يجعل الأشخاص يتوقّفون عن الإساءة إليك. فالحلّ الأفضل هو إخبار شخص راشد لكي يضع حدًّا لهم.

٣و٤- فكّر ماذا ستشعر لو أنّ أحدهم فعل لك الشّيء نفسه. يجب أن لا تسيء إلى الأشخاص أو تهينهم. وإذا وجدت أنّ هذا الأمر قد حصل مع شخص آخر، عليك إخبار شخص راشد لكي يتصرّف بشكل صحيح. تذكّر دائمًا « افعل للآخرين ما تريد أن يفعله الآخرون لك».

٥و ٦- لا يريد أحد نشر صور محرجة له على الإنترنت. وإذا أردت نشر صورة (محرجة كانت أم لا) عليك أوّلا أخذ إذن كلّ من يظهر فيها. وإذا نشر أحدهم صورة محرجة لك من دون إذنك، لا تنفعل بطريقة مبالغة. كن هادئًا واطلب إليه إزالتها. وتذكّر أنّ إزالة الأشياء عن الإنترنت لا يعني محوها نهائيًّا، فمن الممكن أن تكون ما زالت موجودة في مكان ما على الشّبكة، ومن الممكن أن يكون أحدهم قد نسخها وأرسلها إلى ملايين الأشخاص من دون علمك أو أخذ الإذن منك. لذلك فكّر جيّدًا قبل أن تنشر أيّ شيء لأنّ ما تجده مضحكًا اليوم من الممكن أن يحرجك غدًا.

٧- يجب أن لا تزعج أصدقاءك بإرسال دعوات إلى لعبة ما. وإذا أرسلت الدّعوة إلى صديق ولم يقبلها فلا تزعجه بإرسالها مرّة أخرى. فكما لا تريد أن يزعجك الآخرون، عليك ألّا تزعجهم أنت أيضًا.

٨- قبل الانضمام إلى إحدى المجموعات على الشّبكة عليك أن تتأكّد من أنّها لا تسيء إلى الآخرين أو للمعتقدات والأديان أو تروّج لأفكار سياسيّة، متطرّفة، شاذّة، خطيرة تتنافى مع الآداب والأخلاق. مثل: العنصريّة، والعنف، والتّعذيب، وتعاطي المخدّرات، والإرهاب، وممارسة السّحر، وقتل النّفس... وعليك أن تطرح كلّ ما تريده من مواضيع بشرط أن تتقيّد بالتّوجّه الأساسي للصّفحة كي لا تضيّع وقتك ووقت الآخرين.

٩- تذكّر دائمًا: «احترم رأي الآخرين».

١٠- تذكّر دائمًا: « افعل للآخرين ما تريد أن يفعله الآخرون لك» .

١١- تذكّر عند التّواصل مع الآخرين في غرف الدّردشة أنّ كلّ من يتواجد على الشّبكة يستطيع قراءة ما تكتبه إذا أراد، وأنّ كلماتك مكتوبة ومحفوظة في مكان ما، ومن الممكن أن تعود لملاحقتك في يوم ما. يجب أن تكون حذرًا فأنت لا تستطيع أن تتحكّم بمن قد تصل كلماتك إليهم.
تذكّر دائمًا بأنّه ليست لديك أيّة خصوصيّة على الإنترنت. فخصوصيّتك يمكن أن ينتهكها الآخرون. كما أنّ خصوصية الآخرين تعتمد عليك. وعند التّواصل في غرف الدّردشة إعلم أنّه لن يحكم عليك من خلال لونك أو شكلك أو وزنك أو عمرك أو ملابسك وإنّما من نوعيّة كتاباتك.

١٢ و١٣- عند التّكلّم وجهًا لوجه، هناك أكثر من مجرّد كلمات. هناك تعابير الوجه، ولغة الجسد، والإيماءات، وحتّى الطّريقة الّتي تتكلّم بها، كلّها تتضافر لتوصل ما تريد قوله. أمّا على الإنترنت فأنت لا ترى الصّورة كاملة وإنّما فقط مجرّد كلمات. لذا فإنّ التّواصل عبر الإنترنت يمكن أن يكون خادعا. فأحيانًا من الصّعب معرفة ما يعنيه الشّخص الآخر بالضّبط من دون أن تتمكّن من رؤيته أو سماعه. لذلك كن واضحًا بما تكتبه على الإنترنت.
كما أنّ استخدام ال emoticonsو والاختصار يساعدان على التّواصل بطريقة سريعة وسهلة وعلى التّعبير عن شعورنا. فهي مفيدة جدًّا في التّحادث عبر الإنترنت، وتوفّر الكثير من الوقت. ولكن يجب أن لا يتمّ استخدامها كثيرًا لأنّ بعض الأشخاص لا يعرفون معناها لذا حاول التّقيّد دوما باللّغة المعروفة أكثر.

١٤- يجب احترام خصوصيّة الآخرين، وعدم نشر أي شيء من دون أخذ الإذن أوّلًا. واحمِ أصدقاءك ولا تنشر عناوينهم الإلكترونيّة ومعلوماتهم الشّخصيّة على الشّبكة.

١٥- هذه بعض القواعد المهمّة الّتي يجب اتباعها عند إرسال رسائل عبر البريد الإلكتروني:
- كتابة كلّ الأحرف بال majuscule يعني الصّراخ وهذه وقاحة. يجب أن تتحاشى أن تفعل ذلك.
بينما وضع الجملة بين × أو = أو ___ يعني وضع التّعليق بتهذيب واحترام، وأنّ الملاحظة مهمّة جدًّا، وتريد لفت الأنظار إليها. كما يمكنك استخدام ال Bold والItalic .
- لا تفتح أيّة رسالة من شخص لا تعرفه. يجب محوها من دون فتحها.
- لا ترسل أي شيء لست مستعدًّا لقوله وجها لوجه.
- تأكّد أنّ الرّسالة لا تحوي أخطاء إملائيّة.
- يجب دائمًا البدء بالتّحية والانتهاء بالشّكر أو بكلمة لطيفة.
- أكتب دائمًا عنوانًا واضحًا للرّسالة ومناسبًا لمحتواها.
- إذا أردت إرسال رسالة إلى أشخاص عدّة في الوقت نفسه عليك أن تضع العناوين في BCC وذلك احترامًا لخصوصيّتهم. الآخرين.
- إذا وردتك رسالة وأردت إعادة إرسالها إلى أصدقائك عليك أوّلًا أخذ الإذن من مرسلها، ثمّ تأكّد من محو عنوانه الإلكتروني وذلك احترامًا لخصوصيّته.
- لا ترسل رسالة حجمها كبير جدًّا أو نصّها طويل جدًّا. فهل أنت تأخذ وقتًا طويلًا لقراءة رسالة كهذه إذا وصلتك؟
- انتبه أن لا تعيد إرسال كلّ ما يصل إلى بريدك. مثلاً: الرّسائل الّتي تنبئ بحدوث شيء سيّء إذا لم تعد إرسالها.

وثيقة عمل ٢

- أصل كلًّا من هذه ال emoticons بالمعنى المناسب لها:

:+(	مشوّش التّفكير
:~-(	غاضب
;-D	خائف
= O	لا تعليق
:~/	يغمز بعينه ويضحك
{}	يبكي
}{	متفاجئ
;-(	مصدوم
#:-o	وجها لوجه

MOST USED EMOTICONS

=^-.-^= Kitten
^..^ Kitten
@>--->---- Rose
--<--@ Rose
12x--<--@ A dozen roses
:+(Scared
:) Regular smile
:^) Regular smile with a nose
: (Unhappy
: ^(Unhappy
:-P Sticking out tongue
:-s What?!
:-V Shouting
\ ^_^ / Joyful! (Japanese)
:~-(Crying
:~/ Confused
;) Wink
; P Wink
O:-) Angel
:x Kiss
:\' Crying
:^D Happy, approving
:`-(Shedding a tear
:{ Having a hard time
:~) A cold
;(Crying
;-(Angry
;-) Winkey
;-D Winking and laughing
= O Surprised
:-| Indifferent, bored or disgusted
:-|| Very angry
:-~) A cold
:-~| A cold
:.(Crying
:/) Not funny
:> What?
=^* Kisses
@}->-- Rose
O :-) Angel
[] Hug
]:-> Devil
]:-) Happy devil
:-O Open-mouthed, surprised
^5 High five
{} No comment
|(Sleepy (on late night email message)
|-D Big laugh

}: [Angry, frustrated
}{ Face to face
#:-o Shocked
:-6 Exhausted
:-D Laughing
:-e Disappointed
:-i half-smile
%-(Confused
>>:-<< Furious
>-< Furious
>:) Little devil
>:-< Angry
>:-< Mad
>:-(Annoyed
(( )):** Hugs and kisses
((())) Lots of hugging (initials or a name can be put in the middle of the one being hugged)
() Hugging
(:& Angry
(:-& Angry
(:-(Unsmiley
(:-) Smiley variation
(:-* Kiss
(:-\ Very sad
* Kiss
*<:-) Santa Claus
*<|:-) Santa Claus, or a clown
0:-) Angel
12x@>--->--- A dozen roses
8-o Shocked
8-] Wow!
8-| Wide-eyed surprise
: (Sad
) Smile
: [Bored, sad
: | Bored, sad
:( ) Loudmouth, talks all the time; or shouting
:* Kiss
:**: Returning kiss
:,(Crying
:-& Tongue-tied
:-> Smile of happiness
:-< Very sad
:-(Frown
:-) Classic smiley
:-* Kiss

TOP POPULAR TEXT & CHAT ACRONYM

2moro - Tomorrow
2nite - Tonight
10Q - Thank You
ADN - Any Day Now
AFAIK - As Far As I Know
AFK - Away From The Keyboard
ASAP - As Soon As Possible
ATTN - Attention
B/C - Because
B4 - Before
B4N - Bye For Now
BAK - Back At Keyboard
BF - Boy Friend
HYPERLINK “http://www.netlingo.com/word/bff.php”BFF - Best Friends Forever
BRB - Be Right Back
BTW - By The Way
CU - See yoU
CUL - See yoU Later
F2F - Face To Face
FAQ - Frequently Asked Question(s)
FYI - For Your Information
GF - GirlFriend
GTG - Got To Go
GR8 - Great
IC - I See
IK - I Know
ILU - I Love yoU
ILY - I Love You
IMO - In My Opinion
IRL - In Real Life
J/K - Just Kidding
K - oKay
L8R - Later
LMK - Let Me Know
LOL - Laughing Out Loud; Little Old Lady; Lots of Love [minority usage]
N/M - Never Mind
NBD - No Big Deal
NDM - No Disrespect Meant
NP - No Problem
NTG - Not Too Good
OIC - Oh I See
OMG - Oh My God
POV - Point Of View
PPL - PeoPLe
RE - REgarding
RL - Real Life
RT - Real Time
S - *Smile*
TA - Thanks A lot
TC - Telephone Call; Take Care
THX or TX or THKS – Thanks
TMI - Too Much Information
TTYL - Talk To You Later
W8 - Wait
W8ING - Waiting
WB - Welcome Back
XOXO - Hugs and Kisses

٤- لمن هذا؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يحافظ على سمعة رقميّة جيّدة.

الموارد:
- يتعرّف إلى قوانين الملكيّة الفكريّة وحقوق النّسخ والنّشر.

المعارف	المهارات والقدرات	المواقف
• ماهية حقوق الملكية الفكرية.	• يميّز المحتوى الذي يخضع لحقوق الملكية الفكرية.	• يحترم قوانين الملكيّة الفكريّة وحقوق النّسخ والنّشر.

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** ورقة العمل ١ – ورقة العمل ٢ ، كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٥، ١٨، ١٩
- **نمط التّنفيذ:** فردي ومجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق):

- يطلب المعلّم/ة إلى التّلامذة، مسبقًا، أن يحضروا عن الإنترنت معلومات عن شخصيّة ما من اختيارهم من دون كتابة أسمائهم على أوراقهم.

- يجمع الأوراق ويضع علامات عشوائيّة، ثمّ يخلطها ويعيد توزيعها إليهم عشوائيًّا.

- يسأل كلّ من حصل على ورقة ليست له أن يرفع يده. ويقول لهم: ما هي العلامة الّتي حصل عليها كلّ منكم؟ هل تظنّون أنّكم تستحقّون هذه العلامات؟ لمن يجب أن تكون كلّ علامة من هذه العلامات؟ (طبعًا سيجيبون أنّ كلّ شخص يجب أن يحصل على علامة البحث الّذي قدّمه). هل يظنّ كلّ منكم أنّه يجب أن يحصل على علامة البحث الّذي قدّمه؟

- ثمّ يشرح لهم أنّ لا أحدًا منهم يستحقّ علامة على بحثه لأنّ ما كتبه ليس من عمله وإنّما نسخه عن الإنترنت. إذًا هذا النّصّ هو ملك للشّخص الّذي ألّفه، ولا يحقّ لنا الاستفادة منه. وهذا ما يسمّى بحقوق الملكيّة الفكريّة.

مرحلة التّعلّم: (٣٠ دقيقة):

- يطلب المعلّم/ة إلى التّلامذة العمل فرديًّا على حلّ ورقة العمل ١.

- عندما ينهي التّلامذة العمل، يصحّح لهم المعلّم/ة إجاباتهم بشكل جماعي ومن دون مناقشة.

- ثمّ يطلب إليهم العمل بشكل ثنائي لتحديد إذا كان كلّ موقف من هذه المواقف صحيحًا أم غير صحيح.

- عندما ينهي التّلامذة العمل يقرأ المعلّم/ة كلّ موقف على حدة، ثمّ يتناقش معهم حول ما كتبوه.

- أثناء النّقاش يشرح المعلّم/ة للتّلامذة النّقاط الآتية:
  - تخضع الكثير من المعلومات في المواقع إلغاء لحقوق الملكيّة الفكريّة.
  - إذا نسخت عملاً (صور أو فيديو أو موسيقى ....) يخضع لحقوق الملكيّة الفكريّة، وقمت بإعطائه أو بيعه لآخرين، أو نشرته على صفحتك الخاصّة، فأنت تخالف القانون.
  - اذا أردت استخدام أيّ عمل، تذكّر أن تطلب إذنًا من مالكه الأصلي، حتّى لا تتعرّض للملاحقة القانونيّة. وتذكّر أيضًا بأنّه يتوجّب عليك أن تذكر المصدر أو الموقع الّذي أخذت منه هذه المعلومات.

- يمكن للتّلامذة استخدام الصّور أو النّصوص الّتي تخضع لحقوق الملكيّة الفكريّة في التّقارير، والأبحاث المدرسيّة من دون الحصول على إذن. بشرط أن يعيد التّلميذ/ة صياغة الجمل بطريقته الخاصّة، ويضع علامات اقتباس حول أيّة عبارة تستخدم كما هي. ويتوجّب عليه ذكر المصدر أو الموقع الذي أخذت منه هذه المعلومات.

- نسخ كلمة سرّ شخص ما للدّخول إلى أيّ موقع هو عمل مخالف للقانون.

- نسخ البرامج والألعاب غير المجانية وإعطاؤها للأصدقاء، أو نسخ الأفلام هي أعمال مخالفة للقانون أيضًا. ونكون قد حرمنا صانعها الأصلي من حقّ الاستفادة من عمله.

التّطبيق(١٠ دقائق)

- يطلب المعلّم/ة إلى التّلامذة العمل بشكل فرديّ على حلّ ورقة العمل ٢.

- عندما ينهي التّلامذة العمل يقوم المعلّم/ة بالتّصحيح بشكل جماعي.

ورقة عمل ١

- أصل كلّ موقف في العمود الأوّل بما يماثله من العمود الثّاني.

العمود الأوّل	العمود الثّاني
سرقة CD من محل لبيع الموسيقى.	نسخ CD لألعاب غير مجانيّة من أحد أصدقائك.
نسخ مقاطع من بحث صديقك واستخدامها في بحثك.	نسخ صورة أعجبتك عن الإنترنت ووضعها على صفحتك الخاصّة.
نسخ جمل من كتاب لجبران في بحث ما، وذكر اسم الكتاب الّذي أخذتها منه.	نسخ نصّ من موقع الكتروني واستخدامه في بحثك.
سرقة لوحة من معرض والإدعاء أنّك رسمتها	نسخ كلمة سرّ شخص ما، واستخدامها للدّخول إلى موقع معيّن.
أخذ لعبة من محل الألعاب من دون دفع ثمنها.	تحميل أغانٍ من الإنترنت ونسخها لأصدقائي.
أخذ مفتاح منزل الجيران والعبث بمحتوياته في غيابهم.	استخدام جمل أو معلومات أو صور من موقع إلكتروني في بحث ما، وذكر اسم الموقع الّذي أخذتها منهً.

ورقة عمل ٢

- **أجيب بصح أو خطأ عن الجمل الآتية:**

– قانون الملكيّة الفكريّة يسمح لنا باستخدام أيّ محتوى نجده.

– أستطيع استخدام أيّ شيء أجده على الإنترنت.

– أنقل في بحثي المعلومات كلّها من الإنترنت من دون ذكر المصدر.

– أنشر على الإنترنت أيّة صورة أو جملة تعجبني، ولكن أذكر المصدر الّذي أخذتها منه.

– أستطيع سماع الموسيقى وتحميلها من الإنترنت.

٥- هل يحقّ لي فعل ذلك؟

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التلميذ قادرًا على أن يتواصل بشكل آمن عبر الإنترنت، محافظًا على سمعة رقميّة جيّدة، وحاميًا جهازه ومعلوماته الشّخصيّة من الخداع، والاحتيال، والبرمجيّات الخبيثة.

مرحلة الكفاية: يحافظ على سمعة رقميّة جيّدة.

الموارد:
- يحترم قوانين الملكيّة الفكريّة وحقوق النّسخ والنّشر.

المعارف	المهارات والقدرات	المواقف
• ماهية حقوق الملكية الفكريّة.	• يميّز المحتوى الّذي يخضع لحقوق الملكية الفكرية. • يستخدم الطرق المعتمدة لتدوين مصدر المعلومات.	• يحترم قوانين الملكيّة الفكريّة وحقوق النّسخ والنّشر.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٥، ١٨، ١٩
- **نمط التنفيذ:** مجموعات.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق):

- يسمع المعلّم/ة أغنية معروفة إلى التّلامذة، ويصار إلى مناقشة طريقة فعل ذلك معهم. مثال: هل تحميل الأغنية من الإنترنت تصرف صحيح أم لا؟ ولماذا؟ وهل يمكننا وضع الأغنية على أسطوانة وبيعها؟ لماذا؟ أو هل يمكننا استخدام كلماتها في بحثٍ ما؟ ولماذا؟ من يستفيد مادّيًّا من بيع الأغنية؟

مرحلة التعلم: (٤٠ دقيقة):

- يكتب المعلّم/ة كلّ جملة من الجمل الآتية على ورقة صغيرة ثمّ يطويها ويضعها كلّها في علبة.

- يقسّم الصّفّ إلى ١٠ مجموعات، ويطلب إلى كلّ مجموعة سحب ورقة من العلبة، ومناقشة ما كتب فيها وذلك بهدف الإجابة عن الأسئلة الآتية: هل يحقّ لي فعل ذلك أم لا؟ لماذا؟

الجمل هي الآتية:

- عندما تعجبني صورة ما على أيّ موقع كانت أنسخها وأنشرها على صفحتي.
- عندما يطلب إليّ القيام ببحث ما، أبحث عن المعلومات على الإنترنت وأنسخها كما هي.
- عندما يطلب إلي القيامِ ببحث ما، أبحث عن المعلومات على الإنترنت، وآخذ أفكارًا وجملاً من مواقع عدّة ثمّ أرتّبها، وأكتب مقدّمةً مناسبة لموضوع البحث.
- أستخدم صورًا من الإنترنت في بحث للمدرسة.
- لمساعدة صديقي في بحثه أرسل له ما كتبته في بحثي لينسخه أو يستعين به.
- قمت بتحميل بعض الأغاني من الإنترنت، فطلب إليك أصدقاؤك نسخها لهم لأنّ الإنترنت عندهم بطيء، فاستغنمت الفرصة، وبعتهم النّسخ بسعر أقل ممّا لو كانوا يريدون شراء نسخ أصليّة.
- وجدت مقطع فيديو مضحك على موقع ما فنشرته على صفحتك على الإنترنت.
- تستخدم طريقة للعب لعبة بشكل مجّاني على الإنترنت، بينما يدفع الآخرون نقودًا كي يستطيعوا لعبها.
- رأيت أحدهم يكتب كلمة السرّ الخاصة به ليدخل إلى موقع ما، فحفظتها واستخدمتها للدّخول إلى ذلك الموقع.
- وجدت موقعًا على الإنترنت يمكّنك من خلاله تحميل آخر إصدارات الأفلام بشكل مجاني. فقمت بتحميل بعض الأفلام وشاهدتها مع عائلتك في المنزل.

- يعطي المعلّم/ة الوقت الكافي للتّلامذة للعمل، ثمّ يطلب إلى كلّ فريق بدوره، قراءة جملته ومناقشتها مع باقي الصّفّ.

أثناء النّقاش يشرح المعلّم/ة للتّلامذة النّقاط الآتية:

- الكثير من المعلومات في المواقع تخضع لحقوق الملكيّة الفكريّة. كما أنّ الكثير من المواقع تكون مرفقة بصفحة تحدّد ما إذا كان محتواها يخضع لحقوق الملكيّة الفكريّة، وحالات استخدام المحتوى والهدف من ذلك. لذا يجب تّمييز المحتوى المسموح بنسخه واستخدامه والّذي لا يخضع لحقوق الملكيّة الفكريّة، من المحتوى المسموح بنسخه واستخدامه ضمن شروط معيّنة ومن المحتوى الّذي يخضع لحقوق الملكيّة الفكريّة وغير مسموح نسخه واستخدامه أبدا.

- كلّ شخص لديه الحقّ في كسب لقمة العيش من عمله. مثل المصوّرين، والمؤلّفين، والفنّانين، والموسيقيّين، والمبرمجين..... فعندما أنسخ عمل شخص ما، وأستفيد منه، أكون قد حرمت هذا الشّخص من كسب لقمة عيشه. لذا فإنّ مؤلّف العمل أو صانعه هو الشّخص الوحيد الّذي لديه الحقّ بنسخ العمل أو إعطاء إذن لفعل ذلك. والنّسخ من دون إذن يعتبر «سرقة» من قبل قوانين حقوق النّشر.

- إذا نسخت عملا (صور أو فيديو أو موسيقى ....) يخضع لحقوق الملكيّة الفكريّة، وقمت بإعطائه أو بيعه لآخرين، أو نشرته على صفحتك الخاصّة، فأنت تخالف القانون.

- اذا أردت استخدام أيّ عمل، تذكّر أن تطلب إذنًا من مالكه الأصلي، حتّى لا تتعرّض للملاحقة القانونيّة. وتذكّر أيضًا أن تذكر المصدر أو الموقع الّذي أخذت منه هذه المعلومات.

- يمكن للتّلامذة استخدام الصّور أو النّصوص الّتي تخضع لحقوق الملكيّة الفكريّة في التّقارير، والأبحاث المدرسيّة من دون الحصول على إذن. بشرط أن يعيد التّلميذ/ة صياغة الجمل بطريقته الخاصّة، ويضع علامات اقتباس حول أيّة عبارة تستخدم كما هي. ويتوجّب عليه ذكر المصدر أو الموقع الذي أخذت هذه المعلومات منه.
- نسخ كلمة سرّ شخص ما للدّخول إلى أيّ موقع هو عمل مخالف للقانون.

- نسخ البرامج والألعاب غير المجانيّة أو تحميلها وإعطاؤها للأصدقاء، أو نسخ الأفلام هي أعمال مخالفة للقانون أيضًا. ونكون قد حرمنا صانعها الأصلي من حقّ الاستفادة من عمله.

- بإمكاننا ذكر مصدر المعلومات مباشرة بعد المقطع أو الصّورة المستخدمة أو نذكر كلّ المصادر في نهاية البحث.

طرق ذكر المصادر:

- إذا كان مصدر معلوماتنا كتابًا ما، نذكر: اسم المؤلف، عنوان الكتاب، (ثمّ اسم المترجم إذا كان الكتاب مترجمًا)، رقم الجزء (إذا وجد)، الطّبعة، النّاشر، مكان النّشر، سنة النّشر، رقم الصّفحة أو الصّفحات .

- إذا كان مصدر معلوماتنا صحيفة ما، نذكر: اسم الكتاب (إذا وجد)، عنوان المقالة (إذا وجدت)، اسم الصّحيفة، تاريخ العدد، رقم الصّفحة.

- إذا كان مصدر معلوماتنا موقعًا على الإنترنت، نذكر: اسم المؤلف (إذا وجد)، «عنوان الموضوع (إذا وجد)»، <عنوان الموقع>، تاريخ التّحديث الأخير للموقع (أو التّاريخ الّذي أخذنا فيه المعلومات من الموقع).

التّطبيق:

- يطلب المعلّم/ة إلى التّلامذة إيجاد مقطع على الإنترنت حول حقوق الملكيّة الفكريّة ونسخه. ثمّ إعادة صياغته بطريقتهم الخاصّة، وتدوين الموقع الّذي أخذوا منه المعلومات.

- يتمّ تصحيح عملهم ومقارنة ما كتبوه بالنّصّ الأصلي في حصّة لاحقة.

كسول شنيع كريه كسول فاسد بشع قبيح مغفل جاهل غبي كريه مجنون بخيل معيب أبله

الكلام* بيجرح حتى لو كان online

* التنمّر السيبراني هو عندما يُسيء طفل أو مراهق إلى طفل أو مراهق آخر سواء في المدرسة أو خارجها من طريق تخويفه أو إذلاله عبر إرسال تعليقات ورسائل وصور محرجة وعدائية أو نشرها من خلال استخدام الإنترنت أو الهواتف النقالة.

بما أنّني لا أوافق على هذا السلوك غير المقبول، أنا لن أُسيء إلى الآخرين في خلال استخدامي الإنترنت ، لذا:

- انا لن أنشر محتوى أو صورًا محرجة للآخرين.
- انا لن أنشر أيّ تعليق أو أُدوّن أيّ كلام يُسيء إلى أحد أو يجرح مشاعره.
- انا لن أنضمّ إلى المجموعات المسيئة للآخرين أو أُشارك بتأييدها.
- أنا أتجنّب نشر صور مثيرة ومعلومات شخصيّة وحسّاسة تخصّني أو تخصّ أصدقائي على الشبكة مهما كان السبب كي لا يتمّ استغلالها من قبل المتنمّرين أو تشويهها.
- أنا لن أُجاريَ أصدقائي بتصرّفات غير مقبولة .
- أنا لن أردّ على الرسائل المسيئة بل أحفظها كدليل وأُبلّغ شخصًا راشدًا بالأمر كي أحمي نفسي وأحمي غيري.



الإساءة
السّيبيرانيّة

١- أنا شجاع

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحّيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسيّة عند استخدامه أيّ جهاز الكتروني يوفّر خدمة الإنترنت أو الألعاب الالكترونيّة.

مرحلة الكفاية: يتصرّف بوعي ومسؤوليّة مع المضايقات على الإنترنت.

الموارد:
- يتعرّف إلى التّنمّر السّيبيراني.
- يكتشف طرقًا عدّة للتّعامل مع حالات معيّنة من الإساءات على الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهية التّنمّر السّيبيراني. • بعض القواعد الأساسيّة للوقاية من التّنمّر. • وظيفة مكتب جرائم المعلوماتيّة في لبنان.	• يحدّد بعض دوافع التّنمر. • يطبّق بعض الإجراءات الّتي تهدّئ جو الغضب النّاتج عن إساءة أو تنمّر على الشّبكة. • يحتفظ بالرّسائل المسيئة الّتي تلقّاها كدليل لمساعدة ملف الملاحقة لدى مكتب جرائم المعلوماتيّة.	• يحترم مشاعر الآخرين وخصوصيّاتهم. • يتصرّف بوعي في حال تعرّضه للتّنمّر/التّهديد/ الإساءة. • يطلب مساعدة شخص راشد يثق به في حال تعرّضه للتّنمّر/ التّهديد/ الإساءة، وللاستفادة من خدمة الإبلاغ عن الإساءة report abuse المتاحة في معظم المواقع على الإنترنت (استمارة e-helpline على موقع حماية).

- **الفئة المعنيّة:** تلامذة الصّفّين الرّابع والخامس من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١١...١٥-٢٥، لوحة «الكلام بيجرح حتى لو كان online»، فيديو المواطنيّة الرّقميّة، مطويّة الأطفال، صورة بعض أنواع التّنمر.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (١٥ دقيقة):



- يقسّم المعلّم/ة الصّفّ إلى مجموعات عمل، ويطلب إليهم ملاحظة الصّور (المستند ١) بهدف التّعرّف إلى بعض أنواع التّنمّر ومنها إلى تحديد ماهيّة التّنمّر.

- التّنمّر السّيبراني عندما يقوم طفل أو مراهق بالإساءة إلى طفل أو مراهق آخر من طريق إرسال: تهديدات، أو رسائل وصور عدائيّة، أو الإفصاح عن معلومات شخصيّة وحسّاسة، أو تَعمُّد استبعاد الضّحيّة من مجموعة معيّنة على الشّبكة، أو شنّ حملات ضدّه، أو المضايقة، أو الإحراج، أو السّخرية، أو الإهانة وتشويه السّمعة، أو إطلاق إشاعات، أو تشويه الصّور ونشرها عبر المواقع الاجتماعيّة مثل Facebook، غرف الدّردشة، منتديات النّقاش، البريد الإلكتروني، الرّسائل الفوريّة، الهواتف المحمولة، صفحات الويب والمدوّنات Blog... وبعضهم قد يسيء أو يعتدي على الطّفل حتّى يشعر بالإحباط ويفقد احترامه لذاته وثقته بنفسه. ويمكن لأيّ طفل أن يفعل ذلك مع الآخرين كونه يشعر بأنّه محمي وراء الشّاشة.

مرحلة التّعلّم: (٢٥ دقيقة)

- يتوزّع تلامذة الصّفّ على مجموعات عمل.
- تأخذ كلّ مجموعة وثيقة العمل ١، والمستند ١ ويختار أعضاء المجموعة صورة واحدة بالتّوافق.
- يذكرون نوع الإساءة، ويحدّدون طرق التّعامل معها.
- وتتمّ المناقشة جماعيًّا.

نوع الإساءة	طرق التّعامل معها
• التّهديد والصّراخ. • تأييد مجموعة ضدّ أقبح فتاة في المدرسة. • تشويه السّمعة. • تشويه صورة.	١. الاحتفاظ بالأدلّة كالرّسائل، الصّور، الفيديو، التّعليقات، البريد الالكتروني... فقد تدعو الحاجة إليها لاحقًا لإثبات الفعل. ٢. إبلاغ شخص راشد من الأهل أو الأقارب أو المربّين. ٣. صدّ البلطجي block وعدم الرّدّ على أيّ من إساءاته، وتجنّب قراءتها. ٤. الاستفادة من خدمة الإبلاغ عن الإساءة الّتي توفّرها معظم الشّبكات الاجتماعيّة، وخدمات البريد الإلكتروني وغيرها. ٥. التعرّف إلى هويّة المتنمّر ومواجهته...
	ما هو دور مكتب جرائم المعلوماتيّة؟
	أنشىء مكتب مكافحة جرائم المعلوماتيّة وحماية الملكيّة الفكريّة، التّابع لقسم المباحث الجنائية الخاصّة، ضمن وحدة الشّرطة القضائية في المديرية العامّة لقوى الأمن الدّاخلي. وهو يُعنى بمكافحة الجرائم التي تُستخدم فيها التّقنيات المعلوماتيّة العالية وجرائم التّعدّي على الملكيّة الفكريّة. ويتمتّع بصلاحيّات مكافحة الجرائم على الأراضي اللّبنانيّة كافّة. ويتحرّك تلقائيًا في حال الجرم المشهود وفاقًا لمعلومات خاصّة لديه، بعد أخذ إشارة النيابة العامّة المختصّة أو وفاقًا لشكوى محالة منها. الإنترنت.
برأيك، لمَ يعتبر ضرر التّنمّر السّيبيراني كبيرًا؟ • سرعة انتشار المحتوى عبر الشّبكة. • ارتفاع نسبة المشاهدين: لا سيّما إذا كانت الصّفحة تضم عددًا من الأصدقاء وزملاء المدرسة والمعارف والأقارب ما يزيد من حالة الإحراج والإذلال الّتي تشعر بها الضّحيّة. • توافر إمكانيّة الاحتفاظ بالمحتوى: كلّ من وصل إلى المحتوى يستطيع أن يحتفظ به ما يضاعف الضّرر النّفسي والمعنوي الّذي يتعرّض له الطّفل في حال عاود معاينة المحتوى بنفسه أو تمّ إعادة عرضه من قبل آخرين. • الشّبكات الاجتماعيّة: تسمح هذه الشّبكات، من خلال الخدمات الّتي تقدّمها، بشنّ حملات ضدّ شخص معيّن.	

التّطبيق: (١٥ دقيقة)

- كلّ تلميذ يذكر إذا ما تعرّض لإساءة ما، ويقول نوعها، وكيف تصرّف حيال ذلك.

ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

مستند ١


أيّدوا مجموعة أقبح فتاة
LIKE
LIKE
LIKE
LIKE
عرفت أن سالي ارسلت رسالة غرامية إلى وليد؟
حقاً! سأنشر هذا على صفحتي!

وثيقة عمل ١

<table>
<tr><th>نوع الإساءة</th><th>طرق التّعامل معها</th></tr>
<tr><td rowspan="4"></td><td></td></tr>
<tr><td>ما هو دور مكتب جرائم المعلوماتيّة؟</td></tr>
<tr><td></td></tr>
<tr><td colspan="2">برأيك، لِمَ يعتبر ضرر التّنمّر السّيبيراني كبيرًا؟</td></tr>
</table>

٢- أواجه من يسيء إليّ

الكفاية الأولى: : في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحّيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسيّة عند استخدامه أيّ جهاز الكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

مرحلة الكفاية: يتصرّف بوعي ومسؤوليّة مع المضايقات على الإنترنت.

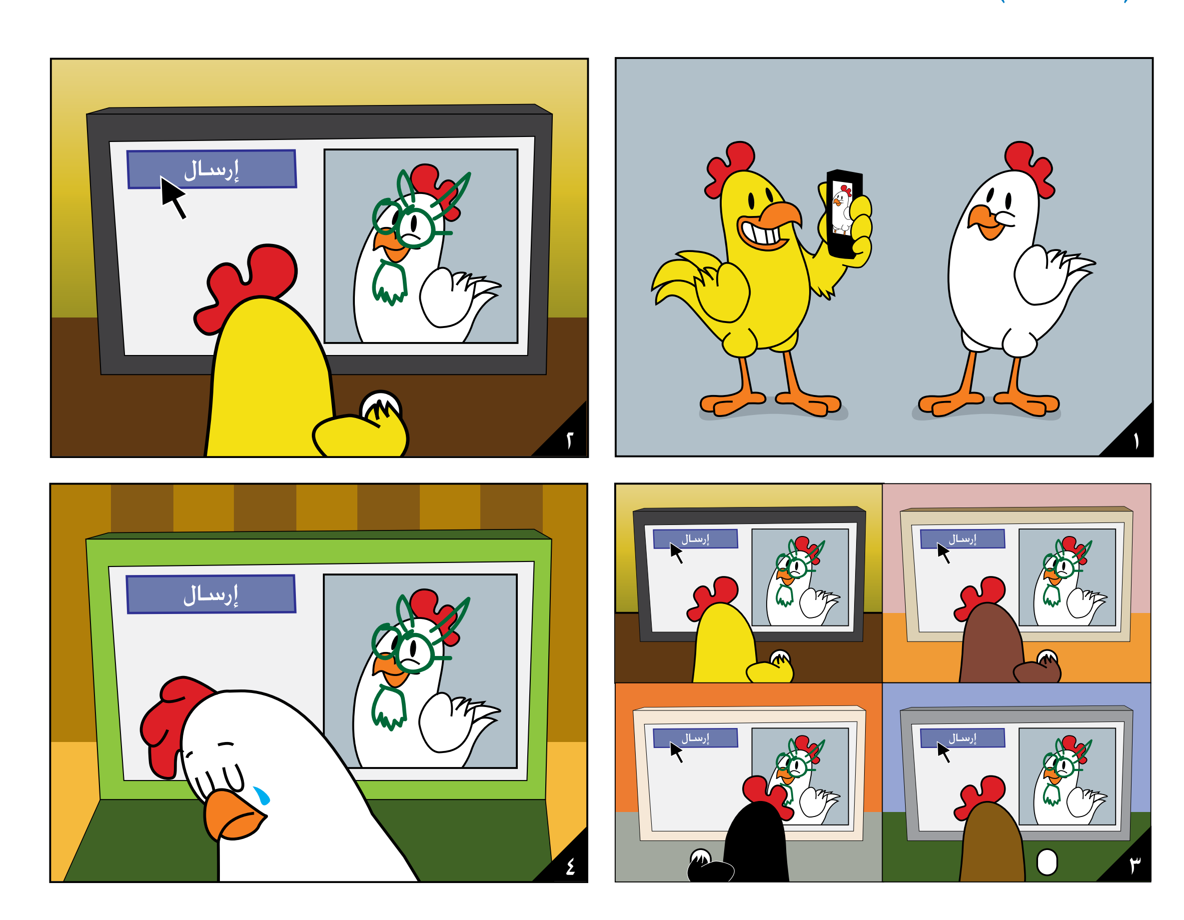
الموارد:
- يتعرّف إلى التّنمّر السّيبيراني.
- يكتشف طرقًا عدّة للتّعامل مع حالات معيّنة من الإساءات على الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهية التّنمّر السّيبيراني. • بعض القواعد الأساسيّة للوقاية من التّنمّر. • مسؤولية المتفرّج ودوره في اتخاذ الإجراءات الإيجابية للتّخفيف من الإساءات والتّنمّر. • وظيفة مكتب جرائم المعلوماتيّة في لبنان. • المحاذير القانونيّة، والعقوبات الّتي تنصّ عليها القوانين الخاصّة بالإنترنت.	• يحدّد بعض دوافع التّنمر. • يطبق بعض الإجراءات الّتي تهدّئ جو الغضب النّاتج عن إساءة أو تنمّر على الشّبكة. • يستخدم خدمة الإبلاغ عن الإساءة report abuse المتاحة في معظم المواقع على الإنترنت (استمارةe-helpline على موقع حماية). • يحتفظ بالرّسائل المسيئة الّتي تلقّاها كدليل لمساعدة ملف الملاحقة لدى مكتب جرائم المعلوماتيّة.	• يحترم مشاعر الآخرين وخصوصيّاتهم. • يتصرّف بوعي في حال تعرّضه للتّنمّر/التّهديد/ الإساءة.

- **الفئة المعنيّة:** تلامذة الصّفّين السّادس والسّابع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **وسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١١...١٥-٢٥، لوحة «الكلام بيجرح حتى لو كان ONLINE»، مطويّة الأطفال، شريط مصوّر صورة الدّجاجة المنشورة، صورة الفتاة في الصّفّ، فيديو المواطنيّة الرّقميّة.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش.
- **المكان** : الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (١٥ دقيقة):



- يقسّم المعلّم/ة الصّفّ إلى مجموعات عمل، ويطلب إليهم ملاحظة الصّور (المستند ١) بهدف إخبار ما حصل مع الدّجاجة وصولاً إلى تحديد ماهيّة التّنمّر.

- التّنمّر السّيبراني عندما يقوم طفل أو مراهق بالإساءة إلى طفل أو مراهق آخر من طريق إرسال: تهديدات، أو رسائل وصور عدائيّة، أو الإفصاح عن معلومات شخصيّة وحسّاسة، أو تَعمُّد استبعاد الضّحيّة من مجموعة معيّنة على الشّبكة، أو شنّ حملات ضدّه، أو المضايقة، أو الإحراج، أو السّخرية، أو الإهانة وتشويه السّمعة، أو إطلاق إشاعات، أو تشويه الصّور ونشرها عبر المواقع الاجتماعيّة مثل Facebook، غرف الدّردشة، منتديات النّقاش، البريد الإلكتروني، الرّسائل الفوريّة، الهواتف المحمولة، صفحات الويب والمدوّنات Blog... وبعضهم قد يسيء أو يعتدي على الطّفل حتّى يشعر بالإحباط ويفقد احترامه لذاته وثقته بنفسه. ويمكن لأيّ طفل أن يفعل ذلك مع الآخرين كونه يشعر بأنّه محمي وراء الشّاشة.

مرحلة التّعلّم: (٣٠ دقيقة)

- يخبر المعلّم/ة التّلامذة ما حصل مع أكرم: نشر عادل صورة لأكرم وهو صغير، وكان يبدو فيها سمينًا جدًّا. فما كان من أكرم إلا أن ردّ له الإساءة بأكبر منها وذلك عبر نشره صورة لعادل لا يرتدي فيها ملابسه.

- يطرح على الجميع السّؤال الآتي: برأيكم ماذا حصل بعد ذلك؟ أو ماكانت النّتيجة بعد ذلك؟

- يتلقّى الإجابات من دون التّعليق عليها.

- يوزّع المعلّم/ة الصّورتين الآتيتين (مستند ٢) لمجموعات العمل ويطلب إليهم الإجابة عن أسئلة وثيقة العمل ١.



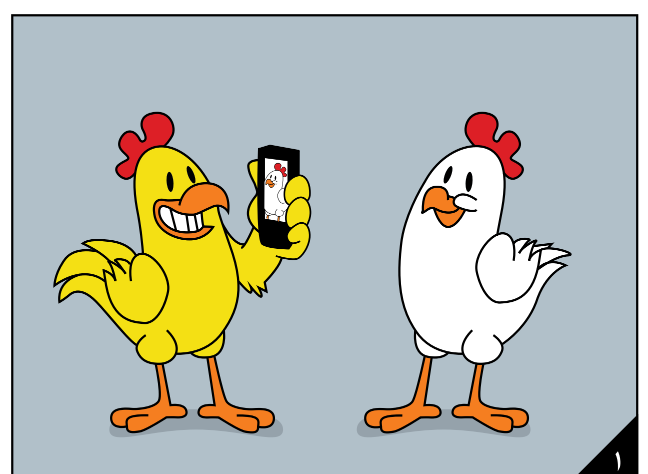


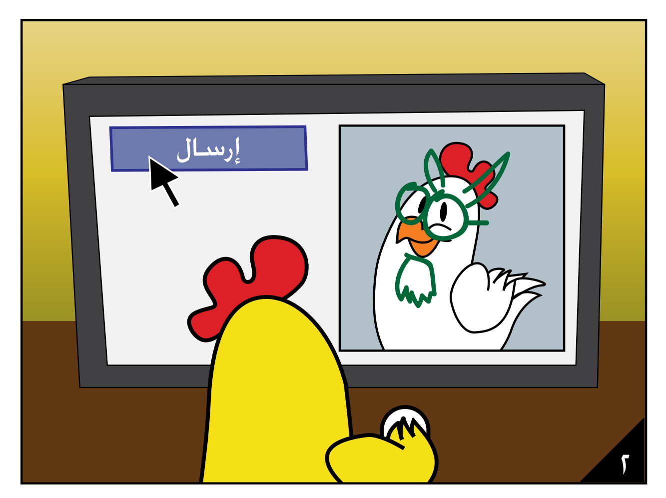
التّطبيق: (١٠ دقائق)

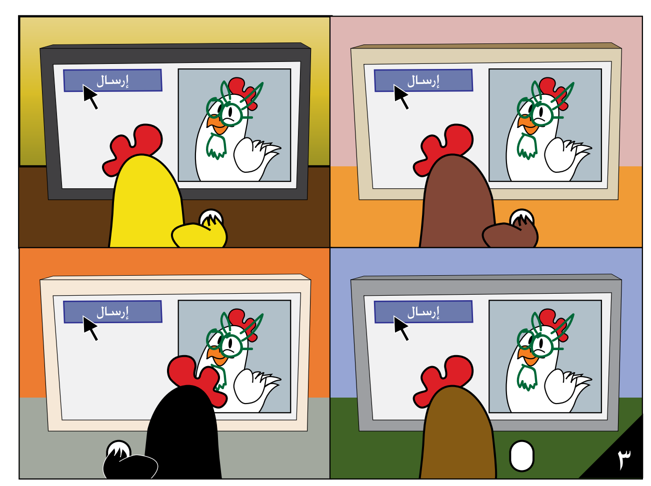
- يعمل التّلامذة إفراديًا على حلّ النّشاط الوارد في الوثيقة ٢، وتتمّ المناقشة جماعيًا.

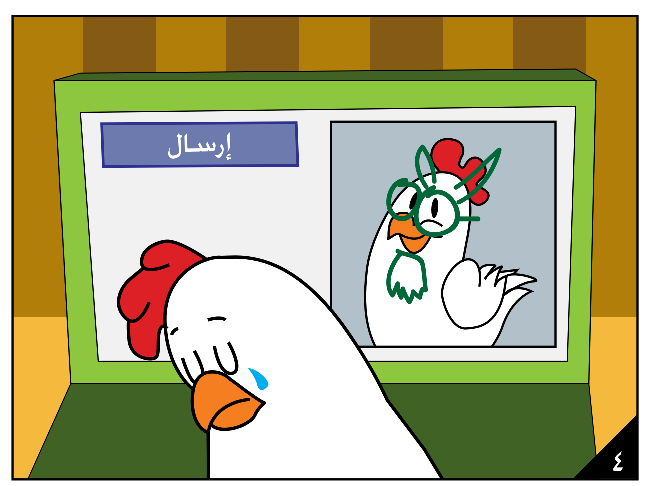
ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

مستند ١









مستند ٢





وثيقة عمل ١

- استنادا إلى ما أراه في الصّورة أملأ الجدول التّالي بما يناسب.

بعض أنواع التّنمّر	كتلميذ كيف أواجه حالات التّنمّر المذكورة
كمعلّم كيف أتصرّف؟	**كمتفرّج ماذا أفعل؟**
لو كنت مكان الأهل كيف أتصرّف؟	

وثيقة عمل ١ (الإجابة)

بعض أنواع التّنمّر	التّشهير، تشويه السّمعة، تشويه الصّور، التّهديد، تأييد مجموعات مسيئة لأحد ما...
كتلميذ/ة كيف أواجه حالات التّنمّر المذكورة	• الاحتفاظ بالأدلّة كالرّسائل، الصّور، الفيديو، التّعليقات، البريد الالكتروني... فقد تدعو الحاجة إليها لاحقًا لإثبات الفعل. • إبلاغ شخص راشد من الأهل أو الأقارب أو المربّين. • صدّ البلطجي block وعدم الرّدّ على أيّ من إساءاته، وتجنّب قراءتها. • الاستفادة من خدمة الإبلاغ عن الإساءة الّتي توفّرها معظم الشّبكات الإجتماعيّة، وخدمات البريد الإلكتروني وغيرها. • التعرّف إلى هويّة البلطجي ومواجهته...
كمعلّم/ة كيف أتصرّف؟	• أحدّث التّلامذة عن التنمر السّيبيراني. • استحدث قوانين وتدابير وعقوبات في النّظام المدرسي لمكافحة التّنمر بأنواعه ومنها السّيبيراني. • أباشر بالتّحقيق الفوري في تقارير التّنمر السّيبيراني. • أعلم أهالي الضّحايا وأهالي المتنمّرين، وأحاول حل المشكلة ضمن حرم المدرسة في حال كان المتنمّر والضّحيّة ينتميان إلى المدرسة نفسها. • أبلغ الشّرطة بالشّك بوجود خطر على الضّحيّة. • أراقب عن كثب سلوك التّلامذة تحسّبًا لاحتمال حدوث تنمر. • أستخدم بعض الدّعم من المرشدين في علم النّفس المتوفّرين في المدرسة.
كمتفرّج/ة ماذا أفعل؟	• أتصرّف بوعي وروية. • لا أنحاز إلى أيّ طرف بل أكون وسيطًا بين الطّرفين. • أطلب إلى الطّرفين أن يتريّثا. • أخفّف من حدّة النّزاع. • أصغي إلى الطّرفين وأحاول إيجاد مخرج للموضوع. • أستدعي الأهل أو أحد الأساتذة في حال لم أجد مخرجا للموضوع.
لو كنت مكان الأهل كيف أتصرّف؟	• لا أتسامح مع التّنمّر في البيت، وأشرح لأطفالي بأنّ أخلاقيّات التّعامل مع النّاس في الحياة الحقيقيّة تنطبق أيضًا على الإنترنت والهواتف المحمولة. • أتحدّث إلى أطفالي عن احترام الآخرين وأوضح لهم بأنّ التّنمّر السّيبيراني هو سلوك سيّء وغير مقبول، وأنّ هناك عواقب وخيمة لمثل هذا السّلوك، سواء أكان في البيت أم في الخارج. • أشجّع أطفالي على أن يكونوا صريحين معي في حال وقوعهم هم أو أيّ شخص من محيطهم ضحيّة التّنمّر السّيبيراني أو أيّ سلوك مزعج على الشّبكة. • أحذّر أطفالي من تشارك كلمة السّرّ أو أيّة معلومات شخصيّة مع أيّ من رفاقه، أو إعارة حاسوبهم الشّخصي أو هواتفهم النّقّالة لأيّ كان منعًا من استغلال المحتوى بهدف الإساءة اليهم. • أشجّع أطفالي على عدم الاستجابة لهذا السّلوك أو الرّدّ عليه. • لا أحذف الرّسائل أو الصّور بل احتفظ بها كأدلّة احتياطيّة. • أحاول التّعرّف إلى الشّخص الّذي قام بهذا الفعل: في حال كان من زملاء المدرسة أو من المعارف فمن الأفضل إعلام أهل البلطجي وحل المشكلة مع الأهل، وأتّصل بالشّرطة في حال الضّرورة أو اكتشاف نوايا سيّئة. • أضع الحاسوب في مكان عامّ في البيت وأحدّد مدّة استخدام الشّبكة والتّوقيت، فالتّنمّر cyber bullying غالبا ما يحدث في وقت متأخّر من اللّيل بعيدا عن الأنظار.

وثيقة عمل ٢

• لكلّ من كارمن ووسام صفحة على الشّبكة. دخلت إلى صفحتهما ولاحظت ما يأتي:

تصّرفات كارمن على صفحتها في الشّبكة	تصرّفات وسام على صفحته في الشّبكة
• نشرت صورًا عائليّة.	• نشر صورة صديقه وعليها بعض الزّخارف المضحكة.
• نشرت صورًا تخصّ صديقتها وهي بملابس السّباحة ومن دون علمها.	• نشر لقطة من فيديو صوّره لزميل له وهو يصرخ بوجه زميل آخر في المدرسة.
• علّقت على صورة إحدى صديقاتها بسخرية.	• علّق بطريقة لطيفة على جملة نشرها صديقه.
• نشرت ما جرى من شجار دار بين صديقتيها.	• نشر صورة تحوي توعية للتّخفيف من التّدخين.
• شاركت في مجموعة شعارها: لا للعنف.	• شارك في مجموعة شعارها: غبّي المدرسة.

أُبدي رأيي بصفحتهما.

٣- أنا أحسن التّصرّف

الكفاية الأولى: : في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسية عند استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الالكترونيّة.

مرحلة الكفاية: يتصرّف بوعي ومسؤوليّة مع المضايقات على الإنترنت.

الموارد:
- يتعرّف إلى التّنمّر السّيبيراني.
- يكتشف طرقًا عدّة للتّعامل مع حالات معيّنة من الإساءات على الإنترنت.

المعارف	المهارات والقدرات	المواقف
• ماهية التّنمّر السّيبيراني. • القواعد الأساسيّة للوقاية من التّنمّر. • مسؤولية المتفرّج ودوره في اتخاذ الإجراءات الإيجابية للتّخفيف من الإساءات والتّنمّر. • وظيفة مكتب جرائم المعلوماتيّة في لبنان. • المحاذير القانونيّة، والعقوبات الّتي تنصّ عليها القوانين الخاصّة بالإنترنت.	• يحدّد بعض دوافع التّنمر. • يطبق بعض الإجراءات الّتي تهدّئ جو الغضب النّاتج عن إساءة أو تنمّر على الشّبكة. • يستخدم خدمة الإبلاغ عن الإساءة report abuse المتاحة في معظم المواقع على الإنترنت (استمارةe-helpline على موقع حماية).	• يحترم مشاعر الآخرين وخصوصيّاتهم. • يتصرّف بوعي في حال تعرّضه للتّنمّر/التّهديد/ الإساءة. • يحتفظ بالرّسائل المسيئة الّتي تلقّاها كدليل لمساعدة ملف الملاحقة لدى مكتب جرائم المعلوماتيّة.

- **الفئة المعنيّة:** تلامذة الصّفّين الثّامن والتّاسع من مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **وسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١١...١٥-٢٥، لوحة «الكلام بيجرح حتى لو كان ONLINE»، فيديو المواطنيّة الرّقميّة، مطويّة الأطفال، صورة الفتاة الّتي تبكي.
- **نمط التّنفيذ:** عمل فردي، عمل مجموعات، نقاش، عصف ذهني.
- **المكان :** الصّفّ أو مختبر المعلوماتيّة أو المكتبة.

سير النّشاط:

التّحفيز (١٥ دقيقة):

- يعرض المعلّم/ة الصّورة الآتية على اللّوح (مستند ١)، ويسأل التّلامذة إبداء تعليقاتهم حول مضمونها.



- يكتب على اللّوح كلمة التّنمر السّيبيراني.
- يطلب إلى التّلامذة ذكر كلّ ما يعرفونه عن هذه الكلمة.
- يكتب الإجابات جميعها على اللّوح ليصار إلى مناقشتها بهدف تحديد أنواع التّنمّر ومنها إلى تحديد ماهيّة التّنمّر.

التّنمّر السّيبراني عندما يقوم طفل أو مراهق بالإساءة إلى طفل أو مراهق آخر من طريق إرسال: تهديدات، أو رسائل وصور عدائيّة، أو الإفصاح عن معلومات شخصيّة وحسّاسة، أو تَعمُّد استبعاد الضّحيّة من مجموعة معيّنة على الشّبكة، أو شنّ حملات ضدّه، أو المضايقة، أو الإحراج، أو السّخرية، أو الإهانة وتشويه السّمعة، أو إطلاق إشاعات، أو تشويه الصّور ونشرها عبر المواقع الاجتماعيّة مثل Facebook، غرف الدّردشة، منتديات النّقاش، البريد الإلكتروني، الرّسائل الفوريّة، الهواتف المحمولة، صفحات الويب والمدوّنات Blogs...
وبعضهم قد يسيء أو يعتدي على الطّفل حتّى يشعر بالإحباط ويفقد احترامه لذاته وثقته بنفسه. ويمكن لأيّ طفل أن يفعل ذلك مع الآخرين كونه يشعر بأنّه محمي وراء الشّاشة.

مرحلة التّعلّم: (٣٠ دقيقة)

- يتوزّع التّلامذة على أربع مجموعات.
- وتعمل كلّ مجموعة على إنجاز المهمّة الموكلة إليها ليصار لاحقًا إلى مناقشة الإجابات جماعيًّا.

المجموعة الأولى تجيب عن الأسئلة الآتية:

- اذكر أنواع الإساءات الّتي تعرفها.
- إذا كتب عأحد شيئًا مسيئًا إليك على الشّبكة ماذا تفعل؟ ولماذا؟
- هل تنشر صورًا محرجة لرفاقك من دون علمهم؟ لماذا؟
- إذا تعرّض أحدهم للإساءة أمامك كيف تتصرّف؟

المجموعة الثّانية تجيب عن الأسئلة الآتية:

- هل تعرف مواقع يمكن اللّجوء إليها في حال التّعرّض للإساءة؟ حدّدها.
- أثناء الدّردشة مع شخص غريب هل تعطيه معلومات شخصيّة عنك؟ لماذا؟
- كيف تتصرّف إذا أنشأ أحد رفاقك مجموعة تسيء إلى أحد ما؟
- هل تستغلّ صورة أحد ما أو تبوح بأسراره إذا قطع صلته بك؟ علّل إجابتك.

المجموعة الثّالثة:

بينما كانت ميرا تدردش مساء مع صديقها، طلب إليها أن ترسل إليه صورة، فما كان من ميرا إلا أن التقطت صورة لها بالكاميرا وأرسلتها إليه. وفي اليوم التّالي بينما كانت متوجّهة إلى الصّفّ سمعت أحدهم يقول لها: «كم هي جميلة قميص النّوم». وآخر يقول لها: «الأسود يليق بك أكثر»، وأخرى تقول لها: «لن أكون صديقتك بعد اليوم».

وعلى الفور عادت ميرا إلى المنزل وحبست نفسها في غرفتها، ولم ترغب بإخبار أحد ما حصل معها لأنّها خافت وارتعبت من العواقب. وتغيّبت عن المدرسة لعدّة أيّام. فجئت لزيارتها وتدخلّت للمساعدة.

- حدّد نوع الإساءة الّتي يمكن أن تكون تعرّضت إليها ميرا.
- اذكر لميرا بعض النّصائح الّتي تمكّنها من التّعامل مع الإساءة الّتي تعرّضت إليها.

المجموعة الرّابعة تملأ الجدول الآتي:

دور الأهل أمام حالات التنمّر	دور المعلّم/ة أمام حالات التنمّر

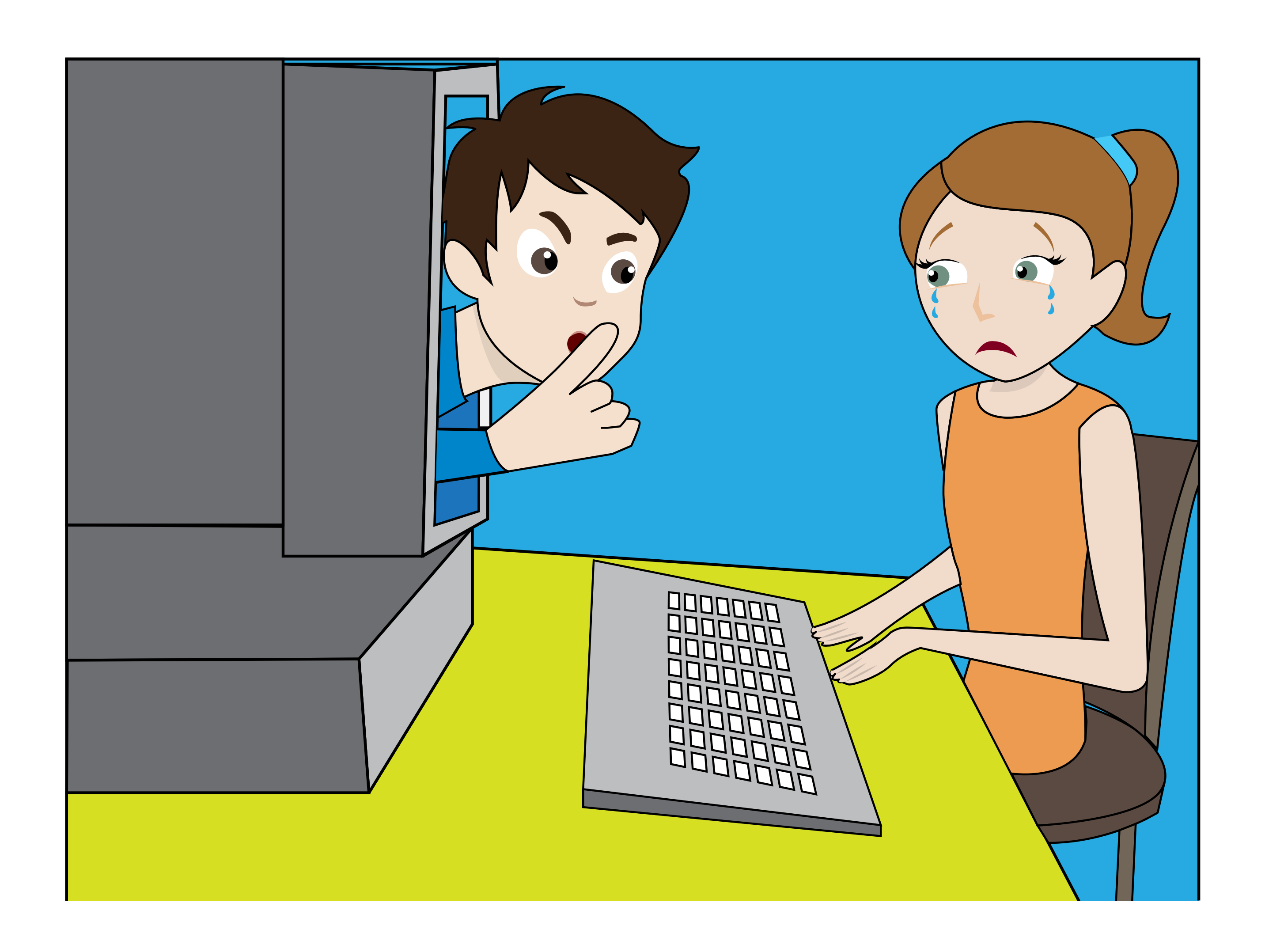
ملاحظة:
الإجابات بمعظمها موجودة في كتاب سلامة الأطفال على الإنترنت.

التّطبيق: (١٠ دقائق)

- يشاهد التّلامذة فيديو الإساءة، ويدون آرائهم حول سبب تصرّف الفتاة على هذا النّحو.
- ما رأيكم بالقول الآتي: «المتنمّر هو شخص أقوى مني، لا أستطيع أن أفعل شيئًا لردعه».

ملاحظة:
في نهاية النّشاط يتمّ عرض مطويّة الأطفال واللّوحة الجداريّة وقراءة ما يتعلّق بمحتوى النّشاط فقط.

مستند ١



وثيقة العمل ١

المجموعة الأولى تجيب عن الأسئلة الآتية:

- أذكر أنواع الإساءات الّتي تعرفها.

....
....
....
....

- إذا كتب أحد شيئًا مسيئًا إليك على الشّبكة ماذا تفعل؟ ولماذا؟

....
....
....
....

- هل تنشر صورًا محرجة لرفاقك من دون علمهم؟ لماذا؟

....
....
....
....

- إذا تعرّض أحدهم للإساءة أمامك كيف تتصرّف؟

....
....
....
....

وثيقة العمل ١

المجموعة الثّانية تجيب عن الأسئلة الآتية:

- هل تعرف مواقع يمكن اللّجوء إليها في حال التّعرّض للإساءة؟ حدّدها.

....

....

....

....

- كيف تتصرّف إذا أنشأ أحد رفاقك مجموعة تسيء إلى أحد ما؟

....

....

....

....

- أثناء الدّردشة مع شخص غريب هل تعطيه معلومات شخصيّة عنك؟ لماذا؟

....

....

....

....

- هل تستغلّ صورة أحد ما أو تبوح بأسراره إذا قطع صلته بك؟ علّل إجابتك.

....

....

....

....

وثيقة العمل ١

المجموعة الثّالثة:

بينما كانت ميرا تدردش مساء مع صديقها، طلب إليها أن ترسل إليه صورة، فما كان من ميرا إلا أن التقطت صورة لها بالكاميرا وأرسلتها إليه. وفي اليوم التّالي بينما كانت متوجّهة إلى الصّفّ سمعت أحدهم يقول لها: «كم هي جميلة قميص النّوم». وآخر يقول لها: «الأسود يليق بك أكثر»، وأخرى تقول لها: «لن أكون صديقتك بعد اليوم».

وعلى الفور عادت ميرا إلى المنزل وحبست نفسها في غرفتها، ولم ترغب بإخبار أحد ما حصل معها لأنّها خافت وارتعبت من العواقب. وتغيّبت عن المدرسة لعدّة أيّام فجئت لزيارتها وتدخلّت للمساعدة.

- حدّد نوع الإساءة الّتي يمكن أن تكون تعرّضت إليها ميرا.

....
....
....
....
....
....

- اذكر لميرا بعض النّصائح الّتي تمكّنها من التّعامل مع الإساءة الّتي تعرّضت إليها.

....
....
....
....
....
....
....

وثيقة العمل ١

المجموعة الرّابعة تملأ الجدول الآتي:

دور الأهل أمام حالات التنمّر	دور المعلّم/ة أمام حالات التنمّر

اعطِ لكل
شـي وقتـو*

* الإدمان على الإنترنت يؤدي إلى اضطراب في السلوك وإلى مشاكل صحية ونفسية منها اضطرابات في النوم، تراجع في المستوى الدراسي والعزلة الاجتماعية، لذا:

- أنا أعرف كيف أُوازن بين الوقت الذي أقضيه على الإنترنت وبين الوقت الذي أقوم فيه بأنشطة أخرى مثل الرياضة، واجباتي المدرسية، تمضية الوقت مع الأصدقاء والعائلة...

- أنا لا أجعل الإنترنت يحل مكان اللقاءات المباشرة مع الأصدقاء والأهل.



الصّحّة والإنترنت

١- صحّتي والإنترنت

الكفاية الأولى: : في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحّيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسيّة عند استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

مرحلة الكفاية: يطبّق قواعد السّلامة الصّحّيّة والنّفسيّة خلال استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

الموارد:
- يتعرّف إلى المحتوى الملائم والمحتوى غير الملائم لنموّه الذّهني والمعرفي.
- يتعرّف إلى الاستخدام الزّائد للإنترنت والقواعد الأساسيّة للتّعامل معها أو تفاديها.
- يحافظ على وضعيّة صحّيّة سليمة أثناء استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الالكترونيّة.

المعارف	المهارات والقدرات	المواقف
• مضمون المحتوى الملائم لعمره. • حالات الاستخدام الزّائد للإنترنت. • طرق معالجة الاستخدام الزّائد للإنترنت. • الوضعيّة الصّحّيّة السّليمة.	• يعدّد بعض مخاطر تصفّح محتوى غير ملائم لعمره. • يسمي بعض حالات الاستخدام الزائد للانترنت. • يذكر التّأثيرات السّلبيّة للاستخدام الزّائد للإنترنت على صحّته النّفسيّة والجسديّة. • يتّخذ وضعية صحّيّة سليمة أثناء استخدامه الإنترنت. • يميّز بين الأجهزة الإلكترونيّة الصّحّيّة وغيرها من الأجهزة.	• يختار بوعي المواقع والألعاب الملائمة لعمره ونموّه الذّهني والمعرفي. • يوازن بين الوقت الّذي يقضيه على الإنترنت وقيامه بأنشطة أخرى. • يحافظ على صحّته (يبقي الصّوت منخفضًا عند استعمال سمّاعات الرّأس، ينظر إلى غرض بعيد موجود في الغرفة أو عبر النّافذة لفترات قصيرة ومتتالية، يتجنّب القضم المتواصل لأغذية غير صحّيّة، ينتبه من الأشعة الصّادرة من الحاسوب والهواتف، والأجهزة الإلكترونيّة المزوّدة بشكل مستمرّ بشبكة الإنترنت ...).

- **الفئة المعنيّة:** تلامذة الصفين الرابع والخامس في مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** : كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٠-١٣-٢٤، والمطويّة، اللّوحة الجداريّة «اعط لكل شي وقتو» ، فيديو المواطنيّة الرّقميّة.
- **نمط التّنفيذ:** عمل مجموعات، نقاش، عمل فردي.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٥ دقيقة) :

- يوزّع المعلّم/ة على التّلامذة الوثيقة رقم ١، ويطلب إليهم حلّ الجزء الأوّل منها بشكل فرديّ.
- ثمّ يوزّع التّلامذة على مجموعات خماسيّة ويطلب إلى كلّ مجموعة حلّ الوثيقة رقم ٢.

مرحلة التّعلّم: (٢٠ دقيقة)

- يعطي المعلّم/ة إلى كلّ مجموعة نسخة عن وثيقة عمل ٣، ويطلب إلى كلّ منها قصّ الصّور والجمل الموجودة في الوثيقة ولصقها على كرتونة كبيرة، واختيار الجمل المناسبة لكلّ صورة، ثم تعلّق الكراتين بعد انتهاء الحصّة على جدار الصّفّ وفي ممرّات المدرسة.
- يطلب إلى المجموعات الإجابة عن أسئلة وثيقة عمل ٤.
- بعد الانتهاء يصار إلى مناقشة الإجابات.
- يطرح المعلّم/ة السّؤالين الآتيين ويفتح مجالًا للمناقشة:
  - كيف نتفادى المواقع غير المفيدة؟
  - هل أنت مع أو ضدّ أن يقوم الأهل بوضع برامج تصفية محتويات وبرامج حماية عائليّة على الإنترنت؟

بعض الإجابات المقترحة عن السّؤال الأوّل:

- تنزيل برامج تصفية محتويات.
- استخدام محرّكات بحث ومواقع خاصّة بالصّغار مثل yahookids، kidsclick، boolify، kidrex . . .
  يفتح المعلّم/ة للتّلامذة مجالًا لتسمية محرّكات البحث الّتي يعرفونها.
- التّأكّد من كتابة عنوان الموقع كما هو.
- عدم فتح أيّة رسالة من مصدر مجهول.
- عدم الضغط على الإعلانات والرّسائل المنبثقة.
- في حال مصادفة أيّ محتوى غير لائق يتمّ إغلاق الشّاشة.

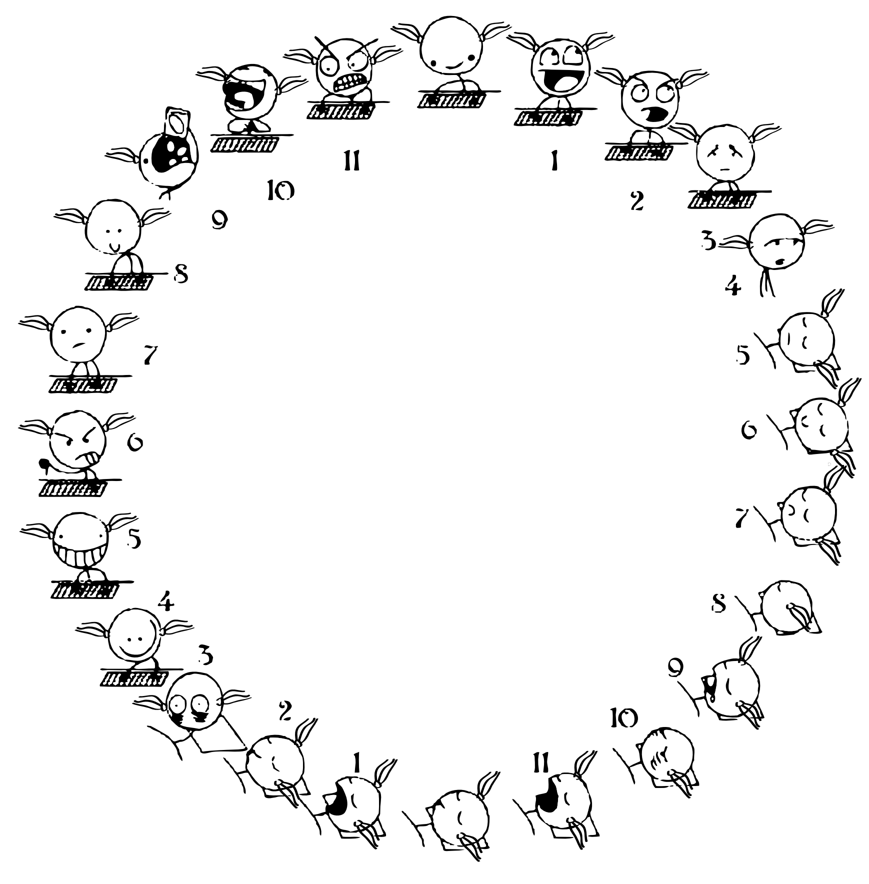
التطبيق (١٥ دقيقة):

- تنفيذ الجزء الثّاني من وثيقة العمل ١ .

ملاحظة:
في نهاية النّشاط يتمّ عرض اللّوحة الجداريّة وقراءة مضمونها.

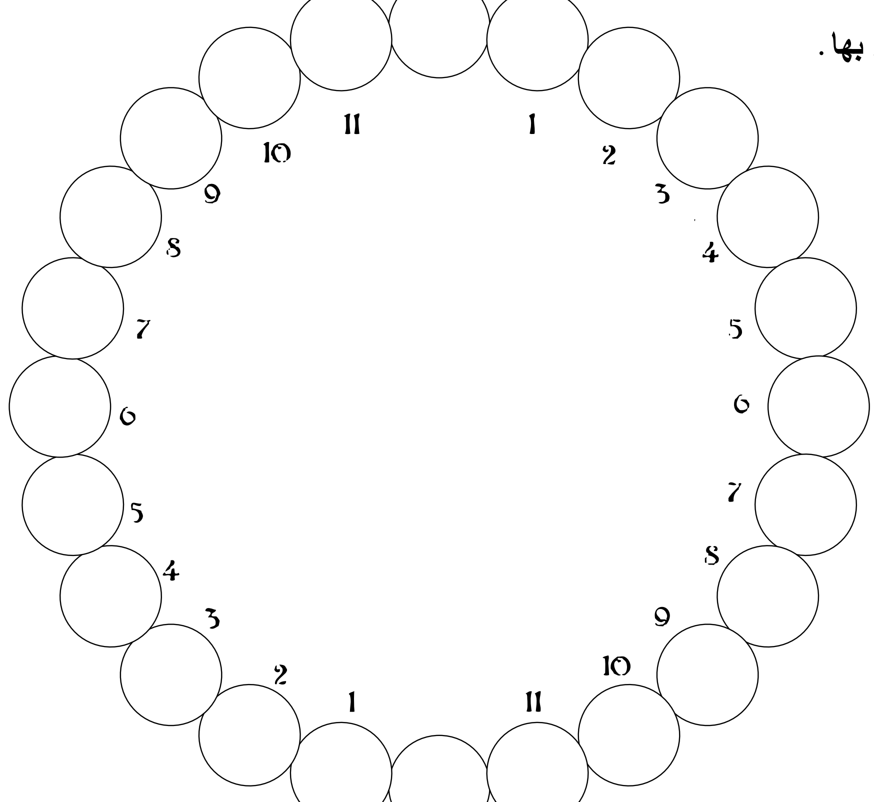
وثيقة العمل ١

الجزء الأوّل:



الجزء الثّاني:

أَذكر عند كلّ دائرة الأنشطة الّتي أقوم بها .



وثيقة العمل ٢

- أكتب في العمود الثّاني ماذا أتوقّع أن يصبح هؤلاء الأشخاص المذكورين في العمود الأوّل عندما يكبرون:

جاد يلعب أربع ساعات يوميًّا على الإنترنت.	
رشا تستخدم الإنترنت للقيام بأبحاث.	
مازن يشاهد صورًا وأفلامًا دمويّة وعنيفة على الإنترنت.	
مروى تدردش كثيرًا على المواقع الاجتماعيّة.	
وسام يتصفّح مواقع غير لائقة.	
رانيا تستخدم مواقع لتعلّم اللّغة الإسبانيّة.	
مروان يستخدم الإنترنت للتّعرّف إلى مختلف الحضارات.	
شادي يعشق لعبة البوكر على الإنترنت.	

وثيقة العمل ٣



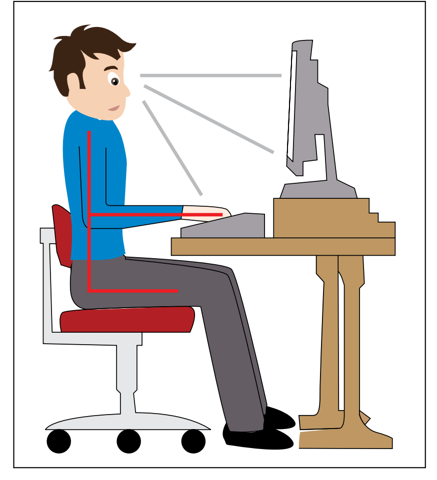














أتّخذ الوضعيّة الصّحيّة السليمة والمناسبة لكلّ جهاز.
أختار المسافة المناسبة للشّاشة للمحافظة على سلامة العيون.
أبقي الصّوت مقبولاً لدى استعمال سمّاعات الرّأس لأنّ الصّوت العالي يؤذي السّمع، ويجعل الشخص قلقًا وعصبيًّا.
أستشير الأهل والطّبيب لدى سماع صفير في الأذن.
أستريح نصف ساعة على الأقلّ كلّما استخدمت الإنترنت لساعتين متواصلتين.
أنظر إلى غرض بعيد موجود في الغرفة أو عبر النّافذة، لفترات قصيرة ومتتالية.
أتوقّف عن تصفّح الإنترنت لممارسة التّمارين الرّياضيّة باستمرار وانتظام.
أتوقّف عن تصفّح الإنترنت للمشاركة بتناول الطّعام مع العائلة أو مع الأصحاب.
لا أنسى الأكل بسبب العمل لساعات طويلة ومتواصلة على الإنترنت.
أنتبه من القضم المتواصل للأغذية غير الصّحّيّة أثناء استخدام الأجهزة الّتي توفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.
أنتبه من الأشعّة الصّادرة من الحاسوب والهواتف والأجهزة الإلكترونيّة المزوّدة بشكل مستمر بشبكة الإنترنت.
لا أنام إلى جانب الحاسوب أو الهواتف والأجهزة الإلكترونيّة.
لا أستخدم الحاسوب في ساعات متأخّرة من اللّيل، فالسّرير مخصّص للنّوم فقط.

وثيقة العمل ٤

أصنّف المواقف الآتية في الجدول:

- تفادي المواقع غير المفيدة.
- يقوم الأهل بوضع برامج تصفية محتويات وبرامج حماية عائليّة على الإنترنت.
- تنزيل برامج وتصفية محتويات.
- استخدام محرّكات بحث ومواقع آمنة.
- التّأكّد من كتابة عنوان الموقع كما هو.
- عدم فتح أيّة رسالة من مصدر مجهول.
- الضّغط على الإعلانات والرّسائل المنبثقة.
- عدم تصفّح محتوى غير لائق.
- مشاهدة صور وأفلام دمويّة وعنيفة على الإنترنت.
- اللّعب لمدّة ساعة يوميًّا على الإنترنت.
- لعب البوكر على الإنترنت.
- الدّردشة كثيرًا على المواقع الاجتماعيّة.

مفيد	غير مفيد	لا موقف

٢- صحّتي والإنترنت

الكفاية الأولى: في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحّيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسيّة عند استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

مرحلة الكفاية: يطبّق قواعد السّلامة الصّحّيّة والنّفسيّة خلال استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونية.

الموارد:
- يميّز المحتوى الملائم والمحتوى غير الملائم لنمّوه الذّهني والمعرفي.
- يتعرّف إلى حالات الاستخدام الزّائد للإنترنت والقواعد الأساسيّة للتّعامل معها أو تفاديها.
- يحافظ على وضعيّة صحّيّة سليمة أثناء استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

المعارف	المهارات والقدرات	المواقف
• مضمون المحتوى الملائم لعمره. • حالات الاستخدام الزّائد للإنترنت. • الوضعيّة الصّحّيّة السّليمة.	• يعدّد بعض مخاطر تصفّح محتوى غير ملائم لعمره. • يسمي بعض حالات الاستخدام الزائد للانترنت. • يتّخذ وضعية صحّيّة سليمة أثناء استخدامه الإنترنت. • يميّز بين الأجهزة الإلكترونيّة الصّحّيّة وغيرها من الأجهزة.	• يختار بوعي المواقع والألعاب الملائمة لعمره ونموه الذّهني والمعرفي. • يوازن بين الوقت الّذي يقضيه على الإنترنت وقيامه بأنشطة أخرى. • يحافظ على صحّته (يبقي الصّوت منخفضًا عند استعمال سمّاعات الرّأس، ينظر إلى غرض بعيد موجود في الغرفة أو عبر النّافذة لفترات قصيرة ومتتالية، يتجنّب القضم المتواصل لأغذية غير صحّيّة، ينتبه من الأشعة الصّادرة من الحاسوب والهواتف، والأجهزة الإلكترونيّة المزوّدة بشكل مستمرّ بشبكة الإنترنت ...).

- **الفئة المعنيّة:** تلامذة الصفين السادس والسابع في مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٠-١٣-٢٤، اللّوحة الجداريّة «اعط لكل شي وقتو»، فيديو إعط لكلّ شي وقتو، وفيديو المواطنيّة الرّقميّة، لعب أدوار.
- **نمط التّنفيذ:** عمل مجموعات، نقاش، عمل فردي.
- **المكان :** الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق) :

- في حال توافرت أداة لعرض الفيديو يقوم المعلّم/ة بعرض فيديو «اعط لكلّ شي وقتو»، وتتمّ المناقشة وصولًا إلى تحديد ما ينتظره التّلامذة من موضوع الحصّة.
- يطلب المعلّم/ة إلى التّلامذة أن يحلّوا وثيقة عمل ١ (مجموعات ثنائيّة).

مرحلة التّعلّم (٢٥ دقيقة) عمل مجموعات:

- يوزّع المعلّم/ة التّلامذة على مجموعات خماسيّة أو سداسيّة، يعطي كلّ مجموعة نسخة عن وثيقة عمل ٢ ونسخة عن وثيقة عمل ٣، يطلب إلى كلّ مجموعة ملء الجدولين الموجودين في الوثيقتين.
- بعد الانتهاء من العمل يصار إلى مناقشة الإجابات.
- يطرح المعلّم/ة السّؤالين الآتيين ويفتح مجالًا للمناقشة:
  ١. كيف نتفادى المواقع غير المفيدة؟
  بعض الإجابات المقترحة عن السّؤال الأوّل:
    - تنزيل برامج تصفية محتويات.
    - استخدام محرّكات بحث ومواقع خاصّة بالصّغار مثل kidsclick، boolify، kidrex، yahookids ... يفتح المعلّم/ة للتّلامذة مجالًا لتسمية محرّكات البحث الّتي يعرفونها.
    - التّأكّد من كتابة عنوان الموقع كما هو.
    - عدم فتح أيّة رسالة من مصدر مجهول.
    - عدم الضغط على الإعلانات والرّسائل المنبثقة.
    - في حال مصادفة أيّ محتوى غير لائق يتمّ إغلاق الشّاشة.
  ٢. هل أنت مع أو ضدّ أن يقوم الأهل بوضع برامج تصفية محتويات وبرامج حماية عائليّة على الإنترنت؟
  ٣. في حال عرض المعلّم/ة الفيديو يسألهم: لو كنت مكان الوالدة في الفيديو هل تتصرّف مثلها؟ لماذا؟

التطبيق (١٥دقيقة):

- يطلب المعلّم/ة إلى كلّ مجموعة أن تنتخب فردًا من أفرادها ليأخذ دور أحد الوالدين، وتقوم المجموعة بمساعدة الفرد المنتخب على اختيار النّصائح والإرشادات للأبناء بشأن كيفيّة الاستفادة من المحتوى الملائم على الإنترنت وكيفية تجنّب المحتوى غير الملائم والمفيد، ثمّ على الفرد أن يمثّل هذا الدّور أمام الصّفّ.

ملاحظة:
في نهاية النّشاط يتمّ عرض اللّوحة الجداريّة وقراءة مضمونها.

وثيقة عمل ١

- أكتب في العمود الثّاني نتيجة ما يفعله كلّ من الأشخاص المذكورين في العمود الأوّل:

جاد يلعب أربع ساعات يوميًّا على الإنترنت.	
رشا تستخدم الإنترنت للقيام بأبحاث.	
مازن يشاهد صورًا وأفلامًا دمويّة وعنيفة على الإنترنت.	
مروى تدردش كثيرًا على المواقع الاجتماعيّة.	
وسام يتصفّح مواقع غير لائقة.	
رانيا تستخدم مواقع لتعلّم اللّغة الإسبانيّة.	
مروان يستخدم الإنترنت للتّعرّف إلى مختلف الحضارات.	
شادي يعشق لعبة البوكر على الإنترنت.	
سالي تأكل الكثير من الحلوى وهي تدردش.	
سارة تنام قرب هاتفها الخلوي المزوّد بالإنترنت.	
غريس تقرّب شاشة الحاسوب من عيونها.	
زينة تشارك أهلها بالأنشطة الّتي يقومون بها.	
كارمن تقوم بحركات رياضيّة عندما تعمل على الحاسوب.	
كايتي تعمل على الحاسوب وهي نائمة.	
لينا ترفع صوت الموسيقى وهي تضع سمّاعات الصّوت.	

وثيقة عمل ٢

- أملأ الجدول الآتي بما يناسب:

الصّورة	مضمون الصّورة	النّتيجة	الحلّ
لا أريد أن أركب الدراجة! أنا مشغول			
لست جائعاً، لا أريد أن أتناول وجبة الغذاء			

الصّورة	مضمون الصّورة	النّتيجة	الحلّ

وثيقة عمل ٣

- أملأ الجدول الآتي بما يناسب:

المحتوى المفيد على الإنترنت	المحتوى غير المفيد على الإنترنت	التّعليل

٣- صحّتي والإنترنت

الكفاية الأولى: : في نهاية مرحلة التّعليم الأساسي، يصبح التّلميذ/ة قادرًا على أن يحمي ذاته من الأخطار (الصّحّيّة والنّفسيّة) مطبّقًا بوعي ومسؤوليّة، قواعد السّلامة الصّحّيّة والنّفسيّة عند استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

مرحلة الكفاية: يطبّق قواعد السّلامة الصّحّيّة والنّفسيّة خلال استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

الموارد:
- يختار المحتوى المفيد والملائم لعمره.
- يتعرّف إلى حالات الاستخدام الزّائد للإنترنت والقواعد الأساسيّة للتّعامل معها أو تفاديها.
- يحافظ على وضعية صحّيّة سليمة أثناء استخدامه أيّ جهاز إلكتروني يوفّر خدمة الإنترنت أو الألعاب الإلكترونيّة.

المعارف	المهارات والقدرات	المواقف
• مضمون المحتوى الملائم لعمره. • حالات الاستخدام الزّائد للإنترنت. • طرق معالجة الاستخدام الزّائد للإنترنت. • الوضعية الصّحّيّة السّليمة.	• يعدّد بعض مخاطر تصفّح محتوى غير ملائم لعمره. • يسمّي حالات الاستخدام الزّائد للإنترنت. • يذكر التّأثيرات السّلبيّة للاستخدام الزّائد للإنترنت على صحّته النّفسيّة والجسديّة. • يتّخذ وضعية صحّيّة سليمة أثناء استخدامه الإنترنت. • يميّز بين الأجهزة الإلكترونيّة الصّحّيّة وغيرها من الأجهزة.	• يختار بوعي المواقع والألعاب الملائمة لعمره ونموه الذّهني والمعرفي. • يوازن بين الوقت الذي يقضيه على الإنترنت وقيامه بأنشطة أخرى. • يحافظ على صحّته (يبقي الصّوت منخفضًا عند استعمال سمّاعات الرّأس، ينظر إلى غرض بعيد موجود في الغرفة أو عبر النّافذة لفترات قصيرة ومتتالية، يتجنّب القضم المتواصل لأغذية غير صحّيّة، ينتبه من الأشعة الصّادرة من الحاسوب والهواتف، والأجهزة الإلكترونيّة المزوّدة بشكل مستمرّ بشبكة الإنترنت ...).

- **الفئة المعنيّة:** تلامذة الصفين الثامن والتاسع مرحلة التّعليم الأساسي.
- **مدّة التّنفيذ:** حصّة كاملة.
- **مستندات ووسائل الإيضاح:** كتاب «الخلفيّة المعرفيّة للمعلّم» ص: ١٠-١٣-٢٤، اللّوحة الجداريّة «اعط لكلّ شي وقتو»، فيديو توعية الأهل ٣، فيديو المواطنيّة الرّقميّة، فيديو إعط لكلّ شي وقتو، وفيديو الجلسة السّليمة فودافون، لعب أدوار.
- **نمط التّنفيذ:** عمل مجموعات، نقاش، عمل فردي.
- **المكان** : الصّفّ.

سير النّشاط:

التّحفيز (١٠ دقائق) :

- يكتب المعلّم/ة القصّة الآتية على اللّوح:
يقوم وليد ورامي ببحث للمدرسة على الإنترنت. دخلا إلى أحد المواقع فتفاجآ بصور غير لائقة.

- ثمّ يوزّع التّلامذة على مجموعات، ويطلب إلى كلّ مجموعة كتابة نهايتين للقصّة، واحدة جيّدة وأخرى غير جيّدة ليصار إلى مناقشتها عند الانتهاء من كتابتها وصولًا إلى تعداد بعض مخاطر تصفّح محتوى غير ملائم لعمرهم، أو دخول مواقع ألعاب غير ملائمة لنموّهم الذّهني والمعرفي.

مرحلة التّعلّم: (٢٥ دقيقة):

في حال توافرت أدوات لعرض الفيديو، يمكن المعلّم/ة تنفيذ النّشاط١:

- يشاهد التّلامذة فيديو فودافون، وعند كلّ طريقة جلوس، يوقف المعلّم/ة الفيديو ويسأل التّلامذة ما هي الأخطاء الّتي ارتكبها الشّخص؟ وماذا تقترحون عليه؟

- عرض فيديو توعية الأهل ومناقشة المضمون، والإجابة عن السّؤال الآتي: لو كنت مكان الأهل كيف تتصرّف؟

- ثمّ يسأل المعلّم/ة التّلامذة عن المواقع الّتي يتصفّحونها على الإنترنت، ونوعيّة المعلومات الّتي يحاولون معرفتها من هذه المواقع. هل يعتبرون أنّ كلّ هذه المواقع تعطي معلومات مفيدة وموثوقة؟ ما هي أنواع المواقع الّتي يمكن أن نجدها على الإنترنت عن طريق الصّدفة أو عن قصد؟ هل يجوز الدّخول إلى كلّ هذه المواقع؟ لماذا؟ يشاهد التّلامذة فيديو «اعطِ لكلّ شي وقتو»، ويجيبون إفراديًّا عن أسئلة عن وثيقة العمل ١، وتتمّ المناقشة جماعيًّا.

في حال عدم توافر أدوات لعرض الفيديو، يمكن المعلّم/ة تنفيذ النّشاط٢:

- يسأل المعلّم/ة التّلامذة عن المواقع الّتي يتصفّحونها على الإنترنت، ونوعيّة المعلومات الّتي يحاولون معرفتها من هذه المواقع. هل يعتبرون أنّ كلّ هذه المواقع تعطي معلومات مفيدة وموثوقة؟ ما هي أنواع المواقع الّتي يمكن أن نجدها على الإنترنت عن طريق الصّدفة أو عن قصد؟ هل يجوز الدّخول إلى كلّ هذه المواقع؟ لماذا؟

- يسأل المعلّم/ة التّلامذة الأسئلة الآتية:
  - هل أنت مع أو ضدّ أن يقوم الأهل بوضع برامج تصفية محتويات وبرامج حماية عائليّة على الإنترنت؟
  - هل أنت مع أو ضدّ أن يقوم الأهل بتحديد قواعد لاستخدام الإنترنت؟
  - لو كنت والدًا/ة ماهي القواعد الّتي تضعها لأولادك بشأن استخدام الإنترنت؟

- يتلقّى المعلّم/ة الإجابات ويُصار إلى مناقشتها جماعيًّا.

التطبيق (١٥ دقيقة):

تجيب كلّ مجموعة عن وثيقة العمل ١، وتتمّ المناقشة جماعيًّا.

ملاحظة:
في نهاية النّشاط يتمّ عرض جداريّة «اعط لكلّ شي وقتو»، وقراءة ما يتعلّق بمحتوى النّشاط فقط.

وثيقة عمل ١

- أملأ الجدول الآتي بما يناسب:

استخدام الإنترنت	
متى يؤثّر على صحّتي النّفسيّة والجسديّة؟	لماذا؟
ما هي تأثيراته على صحّتي النّفسيّة والجسديّة؟	كيف أتفادى هذه الأمور؟
أكتب نصيحة إلى جميع من يستخدم الإنترنت	





الميثاق العائلي لسلامة الأبناء على الإنترنت

اتفاقيّة بين ابن/ابنة...

وأهل...

ميثاق الأهل

يدخل الأولاد إلى شبكة الإنترنت بشكل شبه يومي، يتصفّحون محتويات ما، يتواصلون مع أصدقائهم عبر مواقع التّواصل الاجتماعي، ... وغيرها من الأمور. وبحكم كوني والد/ة، ولأوفّر الرّعاية الشّاملة لأولادي، يكمن دوري في ترشيد استخدام أولادي لهذه الشّبكة ليتمتّعوا بتجربة آمنة ومسلّية. ومسؤوليّتي تقتضي الحفاظ على سلامتهم أثناء استخدامهم لها.

ولمساعدة أولادي على القيام بهذا الدّور، أوافق على اتباع القواعد الآتية:

١- أتعرّف إلى مراكز اهتماماتهم على الشّبكة، ونوعيّة عملهم والمواقع الّتي يزورونها عادة، وأتفقّدها بشكل دوريّ.
٢- أتّفق مع أولادي على قواعد مقبولة لاستخدام الإنترنت كتنظيم وقت استخدامهم للشّبكة والمدّة.
٣- أتحكّم بردّة فعلي إذا أبلغني أحد أولادي عن أيّ شيء سيّء حصل معه على الإنترنت، وأساعده لإيجاد حلّ ومخرج للمشكلة.
٤- أتعرّف إلى الأشخاص الّذين يتواصلون معهم في غرف الدّردشة، والمواقع الاجتماعيّة، والمنتديات وبرامج المراسل الفوري...
٥- أتحدّث إلى أولادي عن أنشطتهم على الشّبكة، وأشاركهم بها.
٦- أضع الحاسوب، ولاسيّما وصلة الإنترنت، في مكان عامّ في المنزل.
٧- أتّفق مع أولادي على طبيعة المواقع المسموح زيارتها، وأزوّدهم بلائحة مواقع آمنة ومفيدة ومناسبة لأعمارهم.
٨- أستخدم برامج وأدوات لتصفية المحتويات وصدّ ما هو غير مناسب لأعمارهم.

التّاريخ:.. توقيع الأهل:..

أفهم أنّ أهلي وافقوا على اتّباع هذه القواعد، وأفهم أنّها ليست مسألة مراقبة ولا مسألة عدم ثقة، وإنّما هي مسألة اهتمام بسلامتي فحسب، شأنها شأن منعي من قيادة الدّرّاجة في أماكن خطرة.

التّاريخ:.. توقيع الابن/الابنة:..

ميثاق الأبناء

أعرف أنّ الإنترنت ممكن أن يكون مكانًا مفيدًا وممتعًا. والمهمّ أن أتبع القواعد الّتي تحميني خلال استخدامي الإنترنت. لذا أنا أوافق على القواعد الآتية:

١. أختار اسم مستخدم وكلمة مرور لا يكشفان عن أيّة معلومات شخصيّة تخصّني أو تخصّ عائلتي.
٢. أحافظ على سرّيّة كلمات المرور الّتي تخصّ حساباتي على الشّبكة، ولا أعطيها إلّا لأهلي.
٣. لا أفتح أيّ حساب إلكتروني من دون علم أهلي أو موافقتهم.
٤. أتجنّب وضع أيّة معلومات شخصيّة، تخصّني أو تخصّ عائلتي، على صفحتي.
٥. أرفض تبادل أيّة معلومات شخصيّة، تخصّني أو تخصّ عائلتي أو أصدقائي، مع أيّ شخص آخر على الإنترنت مثل اسم مدرستي، عنواني، رقم الهاتف، العمر...
٦. أعامل الآخرين خلال استخدامي الإنترنت بالطّريقة نفسها الّتي أرغب أن أعامَل بها.
٧. ألتزم بآداب الحوار والتّواصل عندما أستخدم الإنترنت، بما فيها اختيار الكلمات اللّائقة، وتجنّب استخدام كلمات التّهديد، والكلام الجارح والمخلّ بالآداب.
٨. أصارح أهلي دائما، وأخبرهم عن أيّ شخص أتعرّف إليه على الإنترنت حتّى لو لم يسألوني.
٩. لا أردّ على أيّة رسالة أو بريد إلكتروني مرسل من أيّ شخص أو جهة من دون موافقة أهلي.
١٠. أخبر أهلي، على الفور، إذا تلقّيت رسالة مزعجة أو صورا أو روابط لمواقع تجعلني أشعر بعدم الرّاحة.
١١. أخبر أهلي، على الفور، عن أيّ شخص يزعجني على الإنترنت، أو يرسل إليّ رسائل تحوي عبارات أو صورًا سيّئة ومحرجة.
١٢. لن أتّصل أو ألتقي بأيّ شخص تعرّفت إليه عبر الإنترنت من دون موافقة أهلي ووجودهم.
١٣. أرفض القيام بأيّ فعل يطلبه منّي أيّ شخص إذا كان سيسبّب لي المشاكل، ويزعج أهلي.
١٤. أفهم أنّ أهلي يستخدمون برامج لمراقبة وتصفية المحتويات المزعجة، وذلك لاهتمامهم بحمايتي وليس لمراقبتي.
١٥. أساعد أهلي على اكتشاف أشياء جديدة على الإنترنت وتعلّمها لنتمتّع معًا بتجارب مسلّية.

التّاريخ:................................ توقيع الابن/الابنة:..

أتعهّد بحماية أبنائي أثناء استخدامهم الإنترنت عن طريق التّأكّد من اتباعهم لهذه القواعد. وأتعامل مع أيّ وضع طارئ يبلغوني عنه بإيجابيّة وهدوء ونضج من دون أن ألومهم أو أحرمهم من استخدام الإنترنت.

التّاريخ:................................ توقيع الأهل:..



٦ أنا أحمي حاسوبي الشخصي:

- أنا أستخدم البرمجيات المضادة للفيروسات وأحدّثها دوريًّا.
- أنا أتجاهل وأحذف الرّسائل البريديّة المزعجة أو المجهولة المصدر.
- أنا أُحصّن كلمة السرّ باستخدام ثمانية أرقام على الأقل تجمع ما بين الحروف والأرقام والرموز وأقوم بتغييرها بشكل دوري.
- أنا لن أُحمّل الملفّات (download) أو أنقر على الوصلات (links) أو الملحقات (attachment) إلاّ في حال كنت أثق بالمصدر أو أستشير أحدًا ما.



٧ أنا أُبلّغ عن أيّ شيء مزعج أتعرّض له على الشّبكة:

في خلال استخدامي الشبكة، قد أتلقّى رسائل مزعجة أو رسائل تهديد تجعلني أشعر بعدم الارتياح، في هذه الحال:

- أنا أعلم أنّني لست مخطئًا إن تلقّيت مثل هذه الرّسائل.
- أنا لن أردّ على هذه الرّسائل.
- أنا أُخبر على الفور أهلي أو أيّ شخص راشد أثق به.

مواقع مفيدة باللغة العربية:

www.crdp.org
www.atfalouna.gov.lb/OnlineSafety
www.worldvision.org.lb
www.be-free.info/indexAr.htm
www.safespace.qa/ar/home.aspx

مواقع مفيدة باللغة الفرنسية:

www.e-enfance.org
www.droitsenfant.com/danger.htm
www.internetsanscrainte.fr

مواقع مفيدة باللغة الإنكليزية:

www.microsoft.com/protect
www.getnetwise.org
www.kidproofme.com
www.connectsafely.org
www.netsmartz.org
www.isafe.org
www.staysafe.org
www.facebook.com/HimayaLebanon
twitter.com/OnlineSafetyLeb
www.kafa.org.lb
http://onguardonline.gov

من أجل الإبلاغ عن الشكاوى:

خط الشكاوى التابع لمكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي: ٠١/٢٩٣٢٩٣

من أجل طلب المساعدة:

الاستفادة من خدمة e-helpline التي يوفّرها موقع www.himaya.org






تمتّع على الإنترنت بتجربة آمنة

لكي أتمتّع على الإنترنت بتجربة آمنة، مفيدة ومسليّة... عليّ اتّباع القواعد الآتية:

١ أنا أُحافظ على معلوماتي الشخصيَّة:

كلّ ما يُنشر على الإنترنت يصبح بمتناول الجميع ولا يمكن استرداده، فمن السّهل استغلاله للإساءة إليّ أولتشويهه من قبل الآخرين، لذلك:

- أنا أتجنّب نشر أيّة معلومات شخصيّة تخصّني أو تخصّ عائلتي (اسمي الكامل، عنوان منزلي، صور، عنوان مدرستي...).
- انا لن أُجيب عن أيّة رسالة إلكترونية يُطلب فيها إعطاء معلومات شخصيّة أو مصرفيّة أو رسميّة مهما كانت مغرية.
- أنا أختار اسم مستخدم (Username) وكلمة مرور حيث لا يكشفان عن أيّة معلومات شخصية تخصّني.
- انا أستفيد من أدوات الخصوصيّة (Privacy Settings) للحفاظ على معلوماتي التي لا أريد أن أتشاركها مع الجميع.





٢ أنا أتجنّب الغرباء:

- أنا أرفض التّحدّث إلى الغرباء على الإنترنت لأنّه من السهل انتحال شخصيّة غير حقيقيّة بعمر مزيّف وصورة مزيّفة بغرض الإساءة إليّ.
- أنا لا أُقابل شخصًا غريبًا تعرّفت إليه على الإنترنت إلّا بموافقة أهلي ووجودهم.



٣ أنا أحترم الآخرين وأُحافظ على سمعة رقمية جيدة :

أنا لا أُسيء إلى الآخرين في خلال استخدامي الإنترنت، لذا:

- لن أقوم بكتابة أو تدوين أي تعليق يُسيء إلى أحد أو يجرح مشاعره.
- لن أنشر معلومات شخصيّة على الإنترنت تخصّ الآخرين ومن دون موافقتهم.
- لن أنسخ موسيقى وألعابًا وبرامج بصورة غير قانونية.
- لن أُجاريَ أصدقائي بتصرّفات غير مقبولة .

٤ أنا أتأكّد من صحة المعلومات:

المعلومات الموجودة على الشبكة ليست كلّها صحيحة ومراقبة، لذلك:

- أنا أستند إلى أكثر من مرجع ومصدر.
- أنا أطلب من شخص راشد أثق به أن يتأكّد من صحّتها.



٥ أنا أُوازن بين استخدامي الإنترنت وقيامي بأنشطة أخرى:

- أنا أعرف كيف أُوازن بين الوقت الذي أقضيه على الإنترنت وبين الوقت الذي أقوم فيه بأنشطة أخرى مثل الرياضة، واجباتي المدرسية...
- أنا لا أجعل الإنترنت يحلّ مكان اللّقاءات المباشرة مع الأصدقاء والأهل.



الالتزام بالقواعد الأخلاقيّة على الانترنت:

وذلك من خلال الطّلب إلى الأطفال أن:

- يُحافظوا على سمعة رقميّة جيّدة.
- لا ينشروا محتوى أو صوراً محرجة للآخرين من دون علمهم أو موافقتهم.
- لا يخرقوا قوانين الملكيّة الفكريّة وقواعد الآداب العامة المتعارف عليها اجتماعيّا وأن يستشهدوا بالمصادر بالشّكل الصّحيح.
- لا يقوموا بنشر أو تدوين أي تعليق مسيء للآخرين.
- لا ينضمّوا إلى مجموعات مسيئة للآخرين أو مسيئة للمعتقدات والأديان والتي تروّج لأفكار وقضايا تتنافى مع الأخلاق والآداب مثل العنصرية، العنف، الشيطانية، الإرهاب، السادية، التشجيع على تعاطي المخدرات والانتحار... وأن لا يؤيّدوا هذه المجموعات.

التّعامل مع الإساءة والإبلاغ عنها:

من الضّروري شرح الأمور للأطفال بعمر مبكر وإرشادهم إلى كيفيّة التعامل بشكل صحيح مع الخطر المحتمل، من خلال تحذيرهم أن:

- لا يأخذوا مديح بعض الأشخاص الغرباء على محمل الجدّ.
- لا ينبهروا بوعود الغرباء ولا يمتثلوا لإغراءاتهم: كالمال، والهدايا، والعواطف...
- لا يُجيبوا عن الأسئلة المتعلقة بالبنية الجسدية (القامة، الوزن، لون العينين، السن...).
- لا يشعروا بالرّهبة من الأشياء المريبة وأن يُعلموكم فورًا بذلك.
- المحافظة على سلامتهم على الإنترنت لن توقعهم في مشاكل كحرمانهم من استعمال الحاسوب.

مواقع مفيدة باللغة العربية:

www.crdp.org
www.atfalouna.gov.lb/OnlineSafety
www.tra.gov.lb/Children-protection-AR
www.worldvision.org.lb
www.be-free.info/indexAr.htm
www.safespace.qa/ar/home.aspx

مواقع مفيدة باللغة الفرنسية:

www.e-enfance.org
www.droitsenfant.com/danger.htm
www.internetsanscrainte.fr

مواقع مفيدة باللغة الإنكليزية:

www.microsoft.com/protect
www.kidproofme.com
www.connectsafely.org
www.getnetwise.org
www.netsmartz.org
www.facebook.com/HimayaLebanon
twitter.com/OnlineSafetyLeb
www.kafa.org.lb
http://onguardonline.gov

من أجل الاستعلام عن خدمة الحماية العائلية Family protection على الإنترنت التابعة لـOGERO:

www.ogero.gov.lb

من أجل تحميل برامج تصفية محتويات وبرامج مراقبة أبوية:

www.parentalcontrolbar.org
www.parentalfilter.eu
www.netnanny.com

من أجل الإبلاغ عن الشكاوى:

خط الشكاوى التابع لمكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي: ٠١/٢٩٣٢٩٣





سلامة أطفالنا على الإنترنت



من أجل استخدام سليم وآمن للأطفال على الإنترنت

تُعَدّ شبكة الإنترنت مصدرًا أساسيًّا للمعرفة، وموقعًا مهمًّا لبناء الصّداقات والتّواصل الإجتماعي... وهذا لا يعني بالضّرورة أنّها آمنة، فالصّغار يستخدمون شبكة الإنترنت بحماسة وبطريقة شبه يوميّة ولا يجدون من يرشدهم لتجنّب المخاطر الّتي تنتج من سوء استخدامهم لها.

والجدير بالذّكر أنّ منع الأطفال من استخدام الإنترنت ليس الطريق الأمثل لحمايتهم لذا من المستحسن على الأهل أن يتفقوا مع أطفالهم على النّقاط الآتية:

الحيطة والحذر:

من بديهيّات أو أساسيّات سلامة استخدام الإنترنت:

- عدم إعطاء معلومات شخصيّة مثل الاسم، العمر، المدرسة، العنوان...
- التّأكّد من استخدام أدوات الخصوصيّة (Privacy Settings). على سبيل المثال: عدم تشارك الصّور والمعلومات مع الغرباء.
- الاحتفاظ بسرّيّة كلمة المرور (Password).
- عدم الدّردشة مع الغرباء.
- عدم فتح أو استقبال رسائل بريديّة (E-mails) من الغرباء.
- حضّ الأطفال على إخبار شخصٍ راشد فور شعورهم بعدم الارتياح.

ملاحظة : حاولوا، لو مرّة، استخدام مختلف أنواع محرّكات البحث مثل Google لتعرفوا مقدار المعلومات الموجودة عنكم على الشّبكة.



مراقبة أنشطة الأطفال على الشّبكة والتّحكّم بها:

- استخدام برمجيّات المراقبة الأبويّة (parental control) المتوافرة لحذف المحتويات غير المناسبة ومراقبة المواقع التي يزورها الأطفال ومعرفة ما يفعلونه.

ملاحظة :
- إذا كان الطّفل دون الـ ١٢ سنة من عمره عليكم مرافقته في أثناء استخدامه للإنترنت، وأصرّوا على أن يكون لكم حقّ الدّخول إلى حسابه وبريده الإلكتروني لَتتأكّدوا من عدم توا صله مع الغرباء.
- وإذا كان عمر الطّفل فوق الـ١٢ سنة فشاركوه عالمه من دون رقابة بوليسيّة، وعلّموه كيف يحمي نفسه ويثق بحدسه وذكائه.

- وضع الحاسوب ولا سيّما وصلة الإنترنت في مكانٍ عامّ في المنزل وليس في غرفة نوم الأطفال.
- الاتفاق مع الأطفال على طبيعة المواقع المسموح زيارتها.
- وضع قواعد لاستخدام الإنترنت وذلك من خلال تنظيم أوقات استخدام الشّبكة والمدّة المسموح بها.
- الاتفاق مع الأطفال على مبادئ التّحميل (download) وقواعده: الموسيقى، الأفلام، الألعاب، البرامج ...المسموح بها.

ملاحظة : اختاروا الألعاب مع الأطفال وتأكّدوا من أنها مناسبة لأعمارهم من حيث المضمون، واحذَروا الألعاب التي تتضمّن العنف والمشاهد الدّمويّة لما لها من تأثير سلبيّ في تكوين شخصيّاتهم وسلوكيّاتهم.

الحرص على حماية الحاسوب الشّخصي:

- تأكّدوا من استخدام برامج مكافحة الفيروسات وبرامج الحماية الشّخصيّة مثل برامج جدران النّار (firewall) الموجودة في الحاسوب ... وتحديثها دوريًّا.

فتح باب الحوار والتّواصل:

ويتمّ ذلك من خلال محاورة الأطفال حول:

- مراكز اهتماماتهم على الشّبكة ونوعيّة المواقع التي يزورونها عادةً.
- الأشخاص الّذين يُدردشون معهم على الإنترنت.
- عدم الإنجرار وراء تصرفات أصدقائهم وعدم اعتبار كل ما يقومون به يُعدّ بالضرورة صحيحًا.

ملاحظة :

لا تتصرّفوا بعقليّة القاضي ولا تقوموا بإصدار الأحكام بل تحاوروا مع أطفالكم وكونوا مستعدين لمناقشتهم بطريقة مريحة ومرنة.

